CYBER LAW AND INTELLECTUAL PROPERTY

UNIT1

Introduction to cybercrime

Cybercrime or a computer-oriented crime is a crime that includes a computer and a network. The computer may have been used in the execution of a crime or it may be the target. Cybercrime is the use of a computer as a weapon for committing crimes such as committing fraud, identity theft, or breaching privacy. Cybercrime, especially through the Internet, has grown in importance as the computer has become central to every field like commerce, entertainment, and government. Cybercrime may endanger a person or a nation's security and financial health. Cybercrime encloses a wide range of activities, but these can generally be divided into two categories:

1. Crimes that aim at computer networks or devices. These types of crimes involve different threats (like virus, bugs etc.) and denial-of-service (DoS) attacks.
2. Crimes that use computer networks to commit other criminal activities. These types of crimes include cyber stalking, financial fraud or identity theft.

Classification of Cyber Crime:

1. **Cyber Terrorism –**
   Cyber terrorism is the use of the computer and internet to perform violent acts that result in loss of life. This may include different type of activities either by software or hardware for threatening life of citizens.
   In general, Cyber terrorism can be defined as an act of terrorism committed through the use of cyberspace or computer resources.

2. **Cyber Extortion –**
   Cyber extortion occurs when a website, e-mail server or computer system is subjected to or threatened with repeated denial of service or other attacks by malicious hackers. These hackers demand huge money in return for assurance to stop the attacks and to offer protection.

3. **Cyber Warfare –**
   Cyber warfare is the use or targeting in a battle space or warfare context of computers, online control systems and networks. It involves both offensive and defensive operations concerning to the threat of cyber attacks, espionage and sabotage.

4. **Internet Fraud –**
   Internet fraud is a type of fraud or deceit which makes use of the Internet and could include hiding of information or providing incorrect information for the purpose of deceiving victims for money or property. Internet fraud is not considered a single, distinctive crime but covers a range of illegal and illicit actions that are committed in cyberspace.

5. **Cyber Stalking –**
   This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails. In this case, these stalkers know their victims and instead of offline stalking, they use the Internet to stalk. However, if they

notice that cyber stalking is not having the desired effect, they begin offline stalking along with cyber stalking to make the victims' lives more miserable.

Challenges of Cyber Crime:

1. **People are unaware of their cyber rights-**
   The Cybercrime usually happen with illiterate people around the world who are unaware about their cyber rights implemented by the government of that particular country.

2. **Anonymity-**
   Those who Commit cyber crime are **anonymous** for us so we cannot do anything to that person.

3. **Less numbers of case registered-**
   Every country in the world faces the challenge of cyber crime and the rate of cyber crime is increasing day by day because the people who even don't register a case of cyber crime and this is major challenge for us as well as for authorities as well.

4. **Mostly committed by well educated people-**
   Committing a cyber crime is not a cup of tea for every individual. The person who commits cyber crime is a very **technical** person so he knows how to commit the crime and not get caught by the authorities.

5. **No harsh punishment-**
   In Cyber crime there is no harsh punishment in every cases. But there is harsh punishment in some cases like when somebody commits cyber terrorism in that case there is harsh punishment for that individual. But in other cases there is no harsh punishment so this factor also gives encouragement to that person who commits cyber crime.

Prevention of Cyber Crime:

Below are some points by means of which we can prevent cyber crime:

1. **Use strong password –**
   Maintain different password and username combinations for each account and resist the temptation to write them down. Weak passwords can be easily cracked using certain attacking methods like Brute force attack, Rainbow table attack etc, So make them complex. That means combination of letters, numbers and special characters.

2. **Use trusted antivirus in devices –**
   Always use trustworthy and highly advanced antivirus software in mobile and personal computers. This leads to the prevention of different virus attack on devices.

3. **Keep social media private –**
   Always keep your social media accounts data privacy only to your friends. Also make sure only to make friends who are known to you.

4. **Keep your device software updated –** Whenever you get the updates of the system software update it at the same time because sometimes the previous version can be easily attacked.

5. **Use secure network –** Public Wi-Fi are vulnerable. Avoid conducting financial or corporate transactions on these networks.

6. **Never open attachments in spam emails –** A computer get infected by malware attacks and other forms of cybercrime is via email attachments in spam emails. Never open an attachment from a sender you do not know.
7. **Software should be updated –** Operating system should be updated regularly when it comes to internet security. This can become a potential threat when cybercriminals exploit flaws in the system.

There are three major categories of cyber crimes:

1. Crimes Against People

These crimes include cyber harassment and stalking, distribution of child pornography, credit card fraud, human trafficking, spoofing, identity theft, and online libel or slander.

2. Crimes Against Property

Some online crimes occur against property, such as a computer or server. These crimes include DDOS attacks, hacking, virus transmission, cyber and typo squatting, computer vandalism, copyright infringement, and IPR violations.

3. Crimes Against Government

When a cybercrime is committed against the government, it is considered an attack on that nation's sovereignty. Cybercrimes against the government include hacking, accessing confidential information, cyber warfare, cyber terrorism, and pirated software.

What is Information Security? Information security is the practice of protecting information by mitigating information risks. It involves the protection of information systems and the information processed, stored and transmitted by these systems from unauthorized access, use, disclosure, disruption, modification or destruction. This includes the protection of personal information, financial information, and sensitive or confidential information stored in both digital and physical forms. Effective information security requires a comprehensive and multi-disciplinary approach, involving people, processes, and technology.

Information Security is not only about securing information from unauthorized access. Information Security is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. Information can be a physical or electronic one. Information can be anything like Your details or we can say your profile on social media, your data on mobile phone, your biometrics etc. Thus Information Security spans so many research areas like Cryptography, Mobile Computing, Cyber Forensics, Online Social Media, etc.

During First World War, Multi-tier Classification System was developed keeping in mind the sensitivity of the information. With the beginning of Second World War, formal alignment of the Classification System was done. Alan Turing was the one who successfully decrypted Enigma Machine which was used by Germans to encrypt warfare data.

Effective information security requires a comprehensive approach that considers all aspects of the information environment, including technology, policies and procedures, and people. It also requires ongoing monitoring, assessment, and adaptation to address emerging threats and vulnerabilities.

Why we use Information Security?

We use information security to protect valuable information assets from a wide range of threats, including theft, espionage, and cybercrime. Information security is necessary to ensure the confidentiality, integrity, and availability of information, whether it is stored digitally or in other forms such as paper documents. Here are some key reasons why information security is important:

1. Protecting sensitive information: Information security helps protect sensitive information from being accessed, disclosed, or modified by unauthorized individuals. This includes personal information, financial data, and trade secrets, as well as confidential government and military information.
2. Mitigating risk: By implementing information security measures, organizations can mitigate the risks associated with cyber threats and other security incidents. This includes minimizing the risk of data breaches, denial-of-service attacks, and other malicious activities.
3. Compliance with regulations: Many industries and jurisdictions have specific regulations governing the protection of sensitive information. Information security measures help ensure compliance with these regulations, reducing the risk of fines and legal liability.
4. Protecting reputation: Security breaches can damage an organization's reputation and lead to lost business. Effective information security can help protect an organization's reputation by minimizing the risk of security incidents.
5. Ensuring business continuity: Information security helps ensure that critical business functions can continue even in the event of a security incident. This includes maintaining access to key systems and data, and minimizing the impact of any disruptions.

Information Security programs are build around 3 objectives, commonly known as CIA – Confidentiality, Integrity, Availability.

1. **Confidentiality –** means information is not disclosed to unauthorized individuals, entities and process. For example if we say I have a password for my Gmail account but someone saw while I was doing a login into Gmail account. In that case my password has been compromised and Confidentiality has been breached.
2. **Integrity –** means maintaining accuracy and completeness of data. This means data cannot be edited in an unauthorized way. For example if an employee leaves an organisation then in that case data for that employee in all departments like accounts, should be updated to reflect status to JOB LEFT so that data is complete and accurate and in addition to this only authorized person should be allowed to edit employee data.
3. **Availability –** means information must be available when needed. For example if one needs to access information of a particular employee to check whether

employee has outstanded the number of leaves, in that case it requires collaboration from different organizational teams like network operations, development operations, incident response and policy/change management. Denial of service attack is one of the factor that can hamper the availability of information.

Apart from this there is one more principle that governs information security programs. This is Non repudiation.

- **Non repudiation –** means one party cannot deny receiving a message or a transaction nor can the other party deny sending a message or a transaction. For example in cryptography it is sufficient to show that message matches the digital signature signed with sender's private key and that sender could have a sent a message and nobody else could have altered it in transit. Data Integrity and Authenticity are pre-requisites for Non repudiation.

- **Authenticity –** means verifying that users are who they say they are and that each input arriving at destination is from a trusted source.This principle if followed guarantees the valid and genuine message received from a trusted source through a valid transmission. For example if take above example sender sends the message along with digital signature which was generated using the hash value of message and private key. Now at the receiver side this digital signature is decrypted using the public key generating a hash value and message is again hashed to generate the hash value. If the 2 value matches then it is known as valid transmission with the authentic or we say genuine message received at the recipient side
- **Accountability –** means that it should be possible to trace actions of an entity uniquely to that entity. For example as we discussed in Integrity section Not every employee should be allowed to do changes in other employees data. For this there is a separate department in an organization that is responsible for making such changes and when they receive request for a change then that letter must be signed by higher authority for example Director of college and person that is allotted that change will be able to do change after verifying his bio metrics, thus timestamp with the user(doing changes) details get recorded. Thus we can say if a change goes like this then it will be possible to trace the actions uniquely to an entity.

advantages to implementing an information classification system in an organization's information security program:

1. **Improved security:** By identifying and classifying sensitive information, organizations can better protect their most critical assets from unauthorized access or disclosure.
2. **Compliance**: Many regulatory and industry standards, such as HIPAA and PCI-DSS, require organizations to implement information classification and data protection measures.
3. **Improved efficiency**: By clearly identifying and labeling information, employees can quickly and easily determine the appropriate handling and access requirements for different types of data.
4. **Better risk management**: By understanding the potential impact of a data breach or unauthorized disclosure, organizations can prioritize resources and develop more effective incident response plans.
5. **Cost savings**: By implementing appropriate security controls for different types of information, organizations can avoid unnecessary spending on security measures that may not be needed for less sensitive data.

6. **Improved incident response**: By having a clear understanding of the criticality of specific data, organizations can respond to security incidents in a more effective and efficient manner.

There are some potential disadvantages to implementing an information classification system in an organization's information security program:

1. **Complexity:** Developing and maintaining an information classification system can be complex and time-consuming, especially for large organizations with a diverse range of data types.
2. **Cost**: Implementing and maintaining an information classification system can be costly, especially if it requires new hardware or software.
3. **Resistance to change:** Some employees may resist the implementation of an information classification system, especially if it requires them to change their usual work habits.
4. **Inaccurate classification:** Information classification is often done by human, so it is possible that some information may be misclassified, which can lead to inadequate protection or unnecessary restrictions on access.
5. **Lack of flexibility:** Information classification systems can be rigid and inflexible, making it difficult to adapt to changing business needs or new types of data.
6. **False sense of security**: Implementing an information classification system may give organizations a false sense of security, leading them to overlook other important security controls and best practices.
7. **Maintenance:** Information classification should be reviewed and updated frequently, if not it can become outdated and ineffective.

Uses of Information Security :

Information security has many uses, including:

1. **Confidentiality:** Keeping sensitive information confidential and protected from unauthorized access.
2. **Integrity:** Maintaining the accuracy and consistency of data, even in the presence of malicious attacks.
3. **Availability:** Ensuring that authorized users have access to the information they need, when they need it.
4. **Compliance:** Meeting regulatory and legal requirements, such as those related to data privacy and protection.
5. **Risk management:** Identifying and mitigating potential security threats to prevent harm to the organization.
6. **Disaster recovery:** Developing and implementing a plan to quickly recover from data loss or system failures.
7. **Authentication:** Verifying the identity of users accessing information systems.
8. **Encryption:** Protecting sensitive information from unauthorized access by encoding it into a secure format.
9. **Network security:** Protecting computer networks from unauthorized access, theft, and other types of attacks.
10. **Physical security:** Protecting information systems and the information they store from theft, damage, or destruction by securing the physical facilities that house these systems.

Issues of Information Security :

Information security faces many challenges and issues, including:

1. **Cyber threats:** The increasing sophistication of cyber attacks, including malware, phishing, and ransomware, makes it difficult to protect information systems and the information they store.

2. **Human error:** People can inadvertently put information at risk through actions such as losing laptops or smartphones, clicking on malicious links, or using weak passwords.
3. **Insider threats:** Employees with access to sensitive information can pose a risk if they intentionally or unintentionally cause harm to the organization.
4. **Legacy systems:** Older information systems may not have the security features of newer systems, making them more vulnerable to attack.
5. **Complexity:** The increasing complexity of information systems and the information they store makes it difficult to secure them effectively.
6. **Mobile and IoT devices:** The growing number of mobile devices and internet of things (IoT) devices creates new security challenges as they can be easily lost or stolen, and may have weak security controls.
7. **Integration with third-party systems:** Integrating information systems with third-party systems can introduce new security risks, as the third-party systems may have security vulnerabilities.
8. **Data privacy:** Protecting personal and sensitive information from unauthorized access, use, or disclosure is becoming increasingly important as data privacy regulations become more strict.
9. **Globalization:** The increasing globalization of business makes it more difficult to secure information, as data may be stored, processed, and transmitted across multiple countries with different security requirements

Cyber Offences

Cyber offences are the illegitimate actions, which are carried out in a classy manner where either the computer is the tool or target or both.

Cyber-crime usually includes the following −

- Unauthorized access of the computers
- Data diddling
- Virus/worms attack
- Theft of computer system
- Hacking
- Denial of attacks
- Logic bombs
- Trojan attacks
- Internet time theft
- Web jacking

- Email bombing
- Salami attacks
- Physically damaging computer system.

The offences included in the I.T. Act 2000 are as follows −

- Tampering with the computer source documents.
- Hacking with computer system.
- Publishing of information which is obscene in electronic form.
- Power of Controller to give directions.
- Directions of Controller to a subscriber to extend facilities to decrypt information.
- Protected system.
- Penalty for misrepresentation.
- Penalty for breach of confidentiality and privacy.
- Penalty for publishing Digital Signature Certificate false in certain particulars.
- Publication for fraudulent purpose.
- Act to apply for offence or contravention committed outside India Confiscation.
- Penalties or confiscation not to interfere with other punishments.
- Power to investigate offences.

Example

Offences Under The It Act 2000

Section 65. Tampering with computer source documents

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the being time in force, shall be punishable with imprisonment up to three year, or with fine which may extend up to two lakh rupees, or with both.

Explanation − For the purpose of this section "computer source code" means the listing of programs, computer commands, design and layout and program analysis of computer resource in any form.

Object − The object of the section is to protect the "intellectual property" invested in the computer. It is an attempt to protect the computer source documents (codes) beyond what is available under the Copyright Law

Essential ingredients of the section

Section	Offence	Punishment	Bailability and Congizability
65	Tampering with Computer Source Code	Imprisonment up to 3 years or fine up to Rs 2 lakhs	Offence is Bailable, Cognizable and triable by Court of JMFC.
66	Computer Related Offences	Imprisonment up to 3 years or fine up to Rs 5 lakhs	Offence is Bailable, Cognizable and
66-A	Sending offensive messages through Communication service, etc...	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable and triable by Court of JMFC
66-B	Dishonestly receiving stolen computer resource or communication device	Imprisonment up to 3 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-C	Identity Theft	Imprisonment of either description up to 3 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-D	Cheating by Personation by using computer resource	Imprisonment of either description up to 3 years and /or fine up to Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-E	Violation of Privacy	Imprisonment up to 3 years and /or fine up to Rs. 2 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-F	Cyber Terrorism	Imprisonment extend to imprisonment for Life	Offence is Non-Bailable, Cognizable and triable by Court of Sessions
67	Publishing or transmitting obscene material in electronic form	On first Conviction, imprisonment up to 3 years and/or fine up to Rs. 5 lakh On Subsequent Conviction	Offence is Bailable, Cognizable and triable by Court of JMFC

		imprisonment up to 5 years and/or fine up to Rs. 10 lakh	
67-A	Publishing or transmitting of material containing sexually explicit act, etc... in electronic form	On first Conviction imprisonment up to 5 years and/or fine up to Rs. 10 lakh On Subsequent Conviction imprisonment up to 7 years and/or fine up to Rs. 10 lakh	Offence is Non-Bailable, Cognizable and triable by Court of JMFC
67-B	Publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form	On first Conviction imprisonment of either description up to 5 years and/or fine up to Rs. 10 lakh On Subsequent Conviction imprisonment of either description up to 7 years and/or fine up to Rs. 10 lakh	Offence is Non Bailable, Cognizable and triable by Court of JMFC
67-C	Intermediary intentionally or knowingly contravening the directions about Preservation and retention of information	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable.
68	Failure to comply with the directions given by Controller	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.
69	Failure to assist the agency referred to in sub section (3) in regard interception or monitoring or decryption of any information through any computer resource	Imprisonment up to 7 years and fine	Offence is Non-Bailable, Cognizable.
69-A	Failure of the intermediary to comply with the direction issued for blocking for public access of any information through any computer resource	Imprisonment up to 7 years and fine	Offence is Non-Bailable, Cognizable.
69-B	Intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) in regard monitor and collect traffic data or information through any computer resource for cybersecurity	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable.

70	Any person who secures access or attempts to secure access to the protected system in contravention of provision of Sec. 70	Imprisonment of either description up to 10 years and fine	Offence is Non-Bailable, Cognizable.
70-B	Indian Computer Emergency Response Team to serve as national agency for incident response. Any service provider, intermediaries, data centres, etc., who fails to prove the information called for or comply with the direction issued by the ICERT.	Imprisonment up to 1 year and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable
71	Misrepresentation to the Controller to the Certifying Authority	Imprisonment up to 2 years and/ or fine up to Rs. 1 lakh.	Offence is Bailable, Non-Cognizable.
72	Breach of Confidentiality and privacy	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh.	Offence is Bailable, Non-Cognizable.
72-A	Disclosure of information in breach of lawful contract	Imprisonment up to 3 years and/or fine up to Rs. 5 lakh.	Offence is Cognizable, Bailable
73	Publishing electronic Signature Certificate false in certain particulars	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.
74	Publication for fraudulent purpose	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.

knowingly or intentionally concealing

knowingly or intentionally destroying

knowingly or intentionally altering

knowingly or intentionally causing others to conceal

knowingly or intentionally causing another to destroy

knowingly or intentionally causing another to alter.

This section extends towards the Copyright Act and helps the companies to protect their source code of their programs.

Penalties − Section 65 is tried by any magistrate.

This is cognizable and non-bailable offence.

Penalties − Imprisonment up to 3 years and / or

Fine − Two lakh rupees.

The following table shows the offence and penalties against all the mentioned sections of the I.T. Act −

Compounding of Offences

As per Section 77-A of the I. T. Act, any Court of competent jurisdiction may compound offences, other than offences for which the punishment for life or imprisonment for a term exceeding three years has been provided under the Act.

No offence shall be compounded if −

- *The accused is, by reason of his previous conviction, is liable to either enhanced punishment or to the punishment of different kind; OR*
- *Offence affects the socio economic conditions of the country; OR*
- *Offence has been committed against a child below the age of 18 years; OR*
- *Offence has been committed against a woman.*

The person alleged of an offence under this Act may file an application for compounding in the Court. The offence will then be pending for trial and the provisions of Sections 265-B and 265-C of Cr. P.C. shall apply.

Cyber Crime with mobile and wireless devices

Below are some of the most common types of Wireless and Mobile Device Attacks:

- **SMiShing :**
  Smishing become common now as smartphones are widely used. SMiShing uses Short Message Service (SMS) to send fraud text messages or links. The criminals cheat the user by calling. Victims may provide sensitive information such as credit card information, account information, etc. Accessing a website might result in the user unknowingly downloading malware that infects the device.
- **War driving :**
  War driving is a way used by attackers to find access points wherever they can be. With the availability of free Wi-Fi connection, they can drive around and obtain a very huge amount of information over a very short period of time.
- **WEP attack :**
  Wired Equivalent Privacy (WEP) is a security protocol that attempted to provide a wireless local area network with the same level of security as a wired LAN. Since physical security steps help to protect a wired LAN, WEP attempts to provide similar protection for data transmitted over WLAN with encryption. WEP uses a key for encryption. There is no provision for key management with Wired Equivalent Privacy, so the number of people sharing the key will continually grow. Since everyone is using the same key, the criminal has access to a large amount of traffic for analytic attacks.
- **WPA attack :**
  Wi-Fi Protected Access (WPA) and then WPA2 came out as improved protocols to replace WEP. WPA2 does not have the same encryption problems because an attacker cannot recover the key by noticing traffic. WPA2 is susceptible to

attack because cyber criminals can analyze the packets going between the access point and an authorized user.

- **Bluejacking :**
  Bluejacking is used for sending unauthorized messages to another Bluetooth device. Bluetooth is a high-speed but very short-range wireless technology for exchanging data between desktop and mobile computers and other devices.
- **Replay attacks :**
  In Replay attack an attacker spies on information being sent between a sender and a receiver. Once the attacker has spied on the information, he or she can intercept it and retransmit it again thus leading to some delay in data transmission. It is also known as playback attack.
- **Bluesnarfing :**
  It occurs when the attacker copies the victim's information from his device. An attacker can access information such as the user's calendar, contact list, e-mail and text messages without leaving any evidence of the attack.
- **RF Jamming :**
  Wireless signals are susceptible to electromagnetic interference and radio-frequency interference. Radio frequency (RF) jamming distorts the transmission of a satellite station so that the signal does not reach the receiving station.

Cyber crime against women:-

Internet surfing has become a regular practice for educational, social, entertainment, or professional purposes in today's digital world. Women have been working or learning using online platforms and frequently accessing social media platforms. While most people are engaged on the internet and other digital platforms for various educational and recreational purposes, many miscreants use these digital tools to abuse and bully online users, especially women. This type of criminal activity is called Cybercrime, as it involves using cyberspace. Cybercrime can be defined as unlawful activities conducted through the internet and digital devices intending to creep into the private space of others and disturb them with objectionable content and misbehavior. Cybercrime affects women the most by subjecting them to mental and emotional harassment.

Cyber Violence Against Women:
Cyber violence uses Computer Technology to access women's personal information and use the internet for harassment and exploitation. Women are becoming soft targets as they often trust other people and are unaware of the consequences. Cyber crime has increased because it is difficult to detect and prove and is seldom reported. Cyber crime is away from traditional monitoring, investigation, or audit and requires specialists to understand the nature of the crime. Cyber crime affects women the most by subjecting them to mental and emotional harassment. Most women become distressed, humiliated, and depressed under this type of crime which is challenging to address and resolve.

Types of Cyber Crime:
Cyber crime against women includes gender-based and sexual remarks and activities performed through a computer network or mobile phones, affecting the dignity of women and causing emotional distress. The different types of cyber crime against women are explained as follows:

- **Cyber Stalking:** It includes attempting to contact the women via social networking sites without any legitimate purpose, putting threatening messages

on the chat page, and constantly disturbing the victims with objectionable emails and messages to create mental distress.

- **Cyber Defamation:** This activity involves defaming the victim through blackmailing and disclosing their details or modified pictures. It often involves extorting and seeking sexual favors from the victim.
- **Cyber Hacking:** When asked to click on unauthorised URLs or download apps that leak all their personal information on their phones, the women became victims of cyber hacking. The criminals utilise these details for unauthorised monetary transactions and other unlawful activities.
- **Cyber Bullying**: It is an act of regular harassment and bullying of the victim through the digital communication device by posting abusive and misleading content, pictures, or videos and sending rape and death threats.
- **Pornography**: This criminal activity involves posting morphed images of victims and using them for pornographic purposes, sometimes demanding money to remove them from social networking sites.
- **Cyber Grooming:** In this case, a person builds a relationship with a woman through an online platform and pressurizes her for undue favors or doing sexual acts.

How to Tackle Cyber Crime?

The most important part is to have a thorough knowledge and awareness about privacy and cyber crimes to avoid people being vulnerable to such threats. There must be more education on cyber crimes and online fraud and how to get rid of or handle them. Cyber literacy should start from the basic level with adequate knowledge about good operating practices. It is necessary to remain extra vigilant about cyber privacy and security. Proper awareness and education can help teach good habits and techniques while working online with digital devices. There has been an increasing trend in cyber crime against women involving blackmailing, fake profiles, morphed images, and publishing or transmitting sexually explicit messages online.

Measures that can be taken for Online Safety:

- Keep a watch on irrelevant or fraudulent messages or emails.
- Avoid responding to emails asking for personal information.
- Avoid accessing fraudulent websites or apps that require personal information.
- Take care of the email address and password.
- Use strong and secure passwords and keep on changing regularly.
- Don’t click on unrecognized UPL or download unknown apps.
- Remain updated about cyber laws and policies.

Legal Provisions Related to Cyber Crime Against Women:

All users of cyberspace are subject to specific laws applicable worldwide. Cyber laws deal with legal issues arising from networked computer technology and digital platforms. These laws protect the victims against cyber crimes and help them address the issues and get justice. **The following acts under the Indian Penal Code (IPC, 1860) section 354 mention the following crimes as punishable under the law with rigorous imprisonment and fines.**

- **Section 354A:** Demand for sexual favors or displaying objectionable pictures against a woman’s consent or making sexual remarks and sexual harassment will cause the imprisonment of up to 3 years with fines.
- **Section 354C:** An act of photographing or publishing a picture of a woman engaged in a private act without her consent will lead to imprisonment of 3 to 7 years.

- **Section 354D:** Contacting a woman online and sending irrelevant emails/messages despite the woman's evident disinterest will cause the imprisonment of 5 years with fines.

The Information Technology Act, 2000 also has provisions for punishment under the following sections:

- **Section 66C**-Identify cyber hacking is a punishable offense with imprisonment of 3 years and fines of Rs. 1 lakh.
- **Section 66E-** Deals with the offense of capturing, publishing, or sending pictures of women in circumstances that violate privacy. This causes imprisonment of 3 years.
- **Section 67A-** Makes it illegal to publish and transmit sexually explicit content and is punishable with imprisonment of up to 5 to 7 years.

The Cyber crime Prevention Act of 2012 focuses on preventing and prosecuting offenders involved in cyber crimes like violating privacy, confidentiality, and integrity of information through computer-related criminal activities.

The Indecent Representation of Women (Prohibition) Act regulates and prohibits the indecent representation of women through the media and publications, which also includes the audio-visual media, the content in electronic form, and distribution of material on the Internet, and the portrayal of women over the web.

Procedure For Resolution:

If a woman finds evidence of cyber crimes, she must contact the nearest cyber cell or a police station. A complaint may also be filed through the National cyber crime reporting portal. To file a complaint alleging a cyber-crime, few documents are required, such as a soft copy or hard copy of a web page or emails with abusive contents, sender details, and access mechanism to the networking system. You can also provide a list of suspects as you find suitable.

Government Initiatives To Enhance Cyber-Security In India:

The Cyber Crime Prevention against Women and Children (CCPWC) scheme is introduced to develop effective measures to handle cyber crimes against women and children in India. It allows a cyber crime victim to file a complaint through an online cyber crime reporting platform. The platform also provides details of law enforcement and regulatory agencies at the local and national levels. The CCPWC also conducts awareness programs starting from the school level as a proactive measure to mitigate cyber crimes.

Way Forward to Prevent Cyber Crime:

The most important part is to have a thorough knowledge and awareness about privacy and cyber crimes to avoid people being vulnerable to such threats. There has to be more education on cyber crimes and online fraud and how to get rid of them or handle them. Cyber literacy should start from the basic level with adequate knowledge about good operating practices. It is necessary to remain extra vigilant about cyber privacy and security. Proper awareness and education can help inculcate good habits and practices while working online with digital devices. There is also a need for stricter law enforcement and punishment for offenders. Media interventions for creating public awareness can make an effective contribution in bringing about changes in the attitudes of people towards gender norms.

Important Data About Cyber Crimes Against Women:

- A total of 10,405 cyber-crimes against women were reported in 2020, with an increase of 24%.

- The Information Technology Act of 2000 is the primary law in India dealing with cyber crime.

Conclusion:

In an increasingly technology-dependent world, criminal activities related to electronic and internet platforms tend to increase, with women becoming the soft targets. The legislation must go the extra mile to punish such criminals with strict actions. Technology has its pros and cons that can be applied for either constructive or evil purposes. To combat cyber crime against women, greater awareness and knowledge about cyber practices, privacy protection, and legal support are required.

Cyber Crime against children

The world is getting closer as daily web usage increases. The world wide web may seem like a significant advancement, but unexpectedly, one of its benefits is that it makes the world closer for its users, making it a smaller place to live. But one of its drawbacks is Cybercrime. Cybercrime is any illicit activity that uses a computer as a tool or a target. The problem with Cybercrime is that it is expanding steadily, and many people have fallen victim to fraud, malicious software, hacking, and other forms of Cybercrime. Some people misuse computers and the internet to commit crimes such as web hacking, email bombing, cyber stalking, and cyberpornography.

Internet Crimes Against Children:

In addition to these crimes, criminals also engage in child abuse online, other types of cybercrime such as child exploitation, cyberbullying, possession of child pornography, exposure to harmful content, and many more. Also, it has been observed that young children or teenagers are the primary and easy targets for criminal activity as they are trusting, naive, adventurous, and eager for attention and affection. For instance, the predator might approach a young individual online and form an online friendship based on the same likes, interests, and activities. Gifts and photos could be exchanged as a result of this. The predator tries to gain the child's trust to get what they want from the child. And this is why the government is dedicated to laws, initiatives, and policies to ensure all Indians always have access to an open, trusted, and accountable internet.

According to the NCRB data, the top five states reporting cyber crimes against children are Uttar Pradesh (170), Karnataka (144), Maharashtra (137), Kerala (107), and Odisha (71),

Steps Taken By Indian Government And NCRB:

- In its magazine "**Crime in India**", the National Crime Records Bureau (NCRB) collects and broadcasts statistical information on crimes. The 2020 report is the most recent to be made public. A total of 305 and 1102 cases of cybercrime against children were reported in 2019 and 2020.
- According to the Seventh Schedule of the Indian Constitution, "Police" and "Public Order" are state matters. Through their Law Enforcement Agencies, States and Union Territories (UTs) are mainly in charge of reducing, detecting, investigating, and punishing crimes, including cybercrime (LEAs). These LEAs prosecute offenders under the law's provisions.
- The Central Government supported the efforts of the State Government by providing guidance and financial support through various schemes for their capacity building.

- To take necessary steps to stop the problem and ensure the safety and security of women and young children using online platforms, the Ministry of Women and Child Development raised the issue with the Ministries of Home Affairs (MHA), Electronics and Information Technology (MEITY), and Education.
- The Ministry of Education was asked to give the necessary instruction to the Central Board of Secondary Education (CBSE) for including appropriate cyber safety content in the school curriculum of children and advised the State Governments to do the same through their School Boards to empower children in navigating the online world with proper security.

Measures And Initiatives Taken Against Cybercrime:

1. **The Information Technology (IT) Act,2000** Section 67B imposes severe penalties for publishing, transferring, or accessing internet content containing child sexual abuse.
2. According to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, users of intermediaries are given more control over their safety, and social media platforms are held responsible. These rules mandate the intermediaries adopt a strong grievance redressal procedure, including the timely resolution of the grievance. The intermediaries must notify people of their terms and conditions, which must include a warning not to host, display, upload, change, publish, transmit, update, or share any information that is, among other things, harmful, defamatory, obscene, invades another's privacy, harms children in any way, or is otherwise illegal.
3. To give LEAs structure and ecosystem for fighting cybercrimes in a thorough and coordinated manner, the government established the **Indian Cyber Crime Coordination Centre (14C)** under the Ministry of Home Affairs.
4. On August 18, 2017, the Central Board of Secondary Education (CBSE) released **school rules about using the internet safely and securely.** This circular instructs schools to create comprehensive security policies and install efficient firewalls, filtering, and monitoring software mechanisms on every computer.
5. As an aspect of the project, a **National Cyber Crime Reporting Portal** (www.cybercrime.gov.in) has been established to help the public to report instances of cybercrime, with a particular emphasis on cybercrime against children and women.
6. The conceptualization of the **toll-free number 1930** (formerly 155260) for helping with filing online cyber complaints. As per the information provided by the applicant in the incident report, incidents reported on the national Cyber Crime Reporting Portal are immediately forwarded to the relevant states for further treatment.
7. MHA has taken several actions to raise awareness of Cybercrime, including distributing messages via the Twitter account @cyberdost, radio campaigns, and publishing a Handbook for Adolescents/Students.
8. The Department has asked all Internet Service Providers (ISPs) of Telecommunications to put in place the necessary measures to inform their users about the usage of parental control filters in end-user computers through emails, bills, SMS, Websites, and other means.

Policy Of Protection Of Children From Sexual Offenses Act (POCSO):

Effective measures to stop child abuse are included in the Protection of Children from Sexual Offenses (POCSO) Act. The Act mandates reporting, including kid-friendly tools for capturing testimony and evidence, and ensures that cases are heard fast. It provides a strict legal framework for protecting children from sexual offenses while preserving the best

interests of the kid throughout the whole legal process. It includes a child-friendly system for recording evidence, conducting investigations, and expediting criminal cases via specified Special Courts. Additionally, it contains the legal framework for combating cybercrime, such as child pornography, adultery, cyberstalking, cyberbullying, defamation against children, sexual harassment, grooming, hacking, identity theft, child trafficking online, online extortion, and violation of privacy.

Legal Toolkit for Investigators:

Monitoring the application of the POCSO Act is the responsibility of the National Commission for the Protection of Child Rights (NCPCR). A variety of actions have been taken by the Commission to safeguard the kids against sexual abuse. A POCSO E-button has been created as a ground-breaking project to make it easier for kids to report incidences of sexual abuse to the Commission online.

Another important step made by this Commission is the creation of a "Legal Toolkit for Investigators." The Handbook is anticipated to be a helpful resource for better understanding the virtual world of crime and its impact on the real world by demystifying cybercrime-related regulations in plain language.

Financial Cybercrime

This crime is when you utilize your skills or third party access for the main purpose to get financial profit. Like accessing an e-bank portal in an unauthorized way and make transactions, make e-commerce payments and take goods without permission.

Financial cybercrime can affect companies of all sizes and in all sectors – as well as private individuals – and can have dramatic consequences. But what are the types of attacks motivated by financial gains and how can we prevent these attacks from succeeding.

What is cybercrime in finance?

Cybercrime in finance is the act of obtaining financial gain through profit-driven criminal activity, including identity fraud, ransomware attacks, email and internet fraud, and attempts to steal financial account, credit card, or other payment card information.

In other words: Financial cybercrime includes activities such as stealing payment card information, gaining access to financial accounts in order to initiate unauthorised transactions, extortion, identity fraud in order to apply for financial products, and so on.

The financial services industry is a very lucrative target and is, therefore, heavily impacted by the rise of cyber criminality. However, cyber financial crime also affects all sorts of companies and unsuspecting individuals like you and me.

Everyone may fall victim to credit card skimming, having their virtual wallets targeted, or malware designed to steal your password.

"Nowadays the term "hacker" slowly disappears from the threat landscape and we see an increase of "criminals" who follow the same paths as always, the only difference being they are now cybercriminals. To avoid becoming a victim of financial cybercrime, you must understand that technology will react to the decisions you make–it cannot make decisions for you," – Adrian Constantin Stanila, Head of Cyber Security Incident Response team in Visma.

What are the types of attacks motivated by financial gains?

We have all received the well-known email where some Nigerian prince has died and their barrister is now contacting you, the sole heir, in order to send over a load of cash to you.

It's just one tiny little hiccup: To receive the payment, you need to do a money transfer through the Western union for some strange and obscure reason you might not fully grasp and then you're out on a slippery slope. Sounds familiar? We all know the story, but the plots have become more advanced.

Various social engineering techniques are most often used in order to manipulate victims into providing confidential information. This can be everything from fake emails supposedly sent by Netflix asking you to pay your subscription invoice, to illegitimate replica emails pretending to be from Paypal or iTunes informing you of your monthly invoice–trying to get you to click on a fraudulent link.

Other well-known scams are Bitcoin scams or love scams, where people are targeted through fake profiles on dating sites or popular social media sites to strike up relationships, leading to the scammer asking for money transactions exploiting the victim's feelings.

What are the consequences of financial crimes?

The consequences of a successful attack can be dramatic and have devastating effects on a company. Loss of large sums can impact the whole economy of the company and even lead to bankruptcy in the most severe cases, especially if the company is small.

Reputational damage in the eyes of stakeholders, clients, and the general public is also an unfortunate consequence. When it comes to private individuals, they may experience having their accounts emptied, savings stolen and debts taken up in their name after having their identity stolen.

So, what initiatives can we take to prevent such cybercrimes from succeeding?

How to prevent financial cybercrimes?
Human error is usually why exploits happen, so it goes without saying that training and awareness are important.

As a company, it is also important to focus on awareness so that the employees will be equipped with the knowledge of how they can be tricked in order to change these behaviours. It is also essential to have well-functioning threat intelligence in place, regular vulnerability tests run by the IT security team, and overall good cyber hygiene.

When it comes to you as an individual, try thinking about these things:

- Always be alert and careful when shopping online, making transactions, or signing into your online bank and government portals
- Always make payments and transfers through official sites and be critical of who you're sending money to and why

- Be careful not to click on suspicious links, always verify the sender's identity and if in doubt, ask for a second opinion

Our goal is to be transparent in regards to cybercrime, choosing to share information rather than keeping it quiet. This is a social responsibility approach that we have put upon ourselves as a company, for the greater good of all our customers, partners, and employees.

Raising awareness and running training in cybercrime techniques and consequences are necessary in order to reduce the number of victims. Through sharing our knowledge, expertise, and experience in our digital channels as well as participating in conferences and running awareness campaigns internally, we aim to contribute to the fight against cyber criminality.

Social Engineering: The Attack on Human Brain and Trust

What is Social Engineering?

The best and easiest definition of the term **Social Engineering** is :
"Social engineering is lying to people to get information."

Social engineering is act of manipulating a person to take any action that may or may not be in "target's" best interest. This may include obtaining information, gaining access, or getting target to take a certain action. It is art of manipulating and misleading people. A phone call with a survey or some quick research on Internet can yield a birthday date or anniversary date, and armed with this information. This information is enough to build a password attack list. Plus, a dozen sites offer detailed records of all sorts of personal information on an individual for a mere INR 100 – INR 3000 or more than this. It doesn't involve use of technical hacking techniques. Only thing which is compromised is human brain and trust.

Social Engineering Phases :

There are 7 phases in a total of Social Engineering Attack.

1. **Identifying the goal –**
   First phase consists of Attack formulation and in accordance, identifying target necessary to fulfill goal.
2. **Information gathering –**
   In this phase, social engineers assess and identify potential information sources and begin information gathering and assessment.
3. **Preparation –**
   In this phase, social engineers analyze information and develop an action plan and methodology to begin approaching the target.
4. **Establishing a relationship –**
   In this phase, social engineers establish a line of communication and begin to build a relationship.
5. **Exploit the relationship –**
   In this phase, the target is "prepped". The exploitation stage uses different methods of misleading to evoke right type of emotions and prime the target to right emotional stage.
6. **Debrief –**
   In this phase, social engineer returns to victim and maintains desired emotional state. The goal is that the victim will not feel like anything in relationship was odd, and they will not understand that they have been under attack.

7. **Goal Satisfaction –**
   After a successful social engineering attack, social engineers will exploit information they have gathered. After social engineering attack, the social engineer will either return to the victim for more information or slowly close relationship.

Understanding Social Engineering Attack with Real-world example :

Imagine if you could simply transfer INR 1000 to an investor and see this grow into INR 10,000 without any effort on your behalf? Cyber criminals use basic human emotions of trust and "greed" to convince victims that they really can get something for nothing. A carefully worded baiting email tells victims to provide their bank account information and funds will be transferred the same day.

This is just 1 example, but there are various types of situations and scenarios through which you and your privacy can be compromised within a few seconds.

Emotions used to perform Social Engineering Attack :

1. Fear
2. Greed
3. Curiosity
4. Helpfulness
5. Urgency etc.

How to Stay Protected Against Social Engineering ?

- The most important things you need to be safe from this are education, skepticism, and consistency in training. The education phase consists of understanding different techniques used by social engineers and making sure you give out information online with caution.
- The second matter, skepticism, is about building a state of mind where one can practice smart caution when receiving emails or talking with people online.
- The third thing is most complex to follow through, as to prepare against social engineering attacks, you would need to encounter them in real life as well.
- By using a people-centric approach to security awareness training that uses phishing simulations, engaging and relevant content, and an understanding of human nature – you can stay protected against social engineering attacks.

Unit 2

Cyber Crime and Cyber law

According to Cybersecurity Ventures, the rise in ransomware attacks is expected to cost companies $20 billion by 2021. Nowadays, ransomware attacks are on the rise, and the most common type of attack is phishing. Ransomware attackers can infect victims' PCs with viruses through email phishing and other methods, resulting in data encryption and subsequent ransom demands.

Malwares – Malicious Software

Malware is a software that gets into the system without user consent with an intention to steal private and confidential data of the user that includes bank details and password. They also generates annoying pop up ads and makes changes in system settings

They get into the system through various means:

1. Along with free downloads.
2. Clicking on suspicious link.
3. Opening mails from malicious source.
4. Visiting malicious websites.
5. Not installing an updated version of antivirus in the system.

Types:

1. Virus
2. Worm
3. Logic Bomb
4. Trojan/Backdoor
5. Rootkit
6. Advanced Persistent Threat
7. Spyware and Adware

What is computer virus:

Computer virus refers to a program which damages computer systems and/or destroys or erases data files. A computer virus is a malicious program that self-replicates by copying itself to another program. In other words, the computer virus spreads by itself into other executable code or documents. The purpose of creating a computer virus is to infect

vulnerable systems, gain admin control and steal user sensitive data. Hackers design computer viruses with malicious intent and prey on online users by tricking them.

Symptoms:

- Letter looks like they are falling to the bottom of the screen.
- The computer system becomes slow.
- The size of available free memory reduces.
- The hard disk runs out of space.
- The computer does not boot.

Types of Computer Virus:

These are explained as following below.

1. **Parasitic –**
   These are the executable (.COM or .EXE execution starts at first instruction). Propagated by attaching itself to particular file or program. Generally resides at the start (prepending) or at the end (appending) of a file, e.g. Jerusalem.
2. **Boot Sector –**
   Spread with infected floppy or pen drives used to boot the computers. During system boot, boot sector virus is loaded into main memory and destroys data stored in hard disk, e.g. Polyboot, Disk killer, Stone, AntiEXE.
3. **Polymorphic –**
   Changes itself with each infection and creates multiple copies. Multipartite: use more than one propagation method. >Difficult for antivirus to detect, e.g. Involutionary, Cascade, Evil, Virus 101., Stimulate.
   Three major parts: Encrypted virus body, Decryption routine varies from infection to infection, and Mutation engine.
4. **Memory Resident –**
   Installs code in the computer memory. Gets activated for OS run and damages all files opened at that time, e.g. Randex, CMJ, Meve.
5. **Stealth –**
   Hides its path after infection. It modifies itself hence difficult to detect and masks the size of infected file, e.g. Frodo, Joshi, Whale.
6. **Macro –**
   Associated with application software like word and excel. When opening the infected document, macro virus is loaded into main memory and destroys the data stored in hard disk. As attached with documents; spreads with those infected documents only, e.g. DMV, Melissa, A, Relax, Nuclear, Word Concept.
7. **Hybrids –**
   Features of various viruses are combined, e.g. Happy99 (Email virus).

Worm:

A worm is a destructive program that fills a computer system with self-replicating information, clogging the system so that its operations are slowed down or stopped.

Types of Worm:

1. **Email worm –** Attaching to fake email messages.
2. **Instant messaging worm –** Via instant messaging applications using loopholes in network.
3. **Internet worm –** Scans systems using OS services.
4. **Internet Relay Chat (IRC) worm –** Transfers infected files to web sites.
5. **Payloads –** Delete or encrypt file, install backdoor, creating zombie etc.
6. **Worms with good intent –** Downloads application patches.

Logical Bomb:

A logical bomb is a destructive program that performs an activity when a certain action has

occurred. These are hidden in programming code. Executes only when a specific condition is met, e.g. Jerusalem.

Script Virus:

Commonly found script viruses are written using the Visual Basic Scripting Edition (VBS) and the JavaScript programming language.

Trojan / Backdoor:

Trojan Horse is a destructive program. It usually pretends as computer games or application software. If executed, the computer system will be damaged. Trojan Horse usually comes with monitoring tools and key loggers. These are active only when specific events are alive. These are hidden with packers, crypters and wrappers.< Hence, difficult to detect through antivirus. These can use manual removal or firewall precaution.

RootKits:

Collection of tools that allow an attacker to take control of a system.

- Can be used to hide evidence of an attacker's presence and give them backdoor access.
- Can contain log cleaners to remove traces of attacker.
- Can be divided as:
  – Application or file rootkits: replaces binaries in Linux system
  – Kernel: targets kernel of OS and is known as a loadable kernel module (LKM)
- Gains control of infected m/c by:
  – DLL injection: by injecting malicious DLL (dynamic link library)
  – Direct kernel object manipulation: modify kernel structures and directly target trusted part of OS
  – Hooking: changing applicant's execution flow

Advanced Persistent Threat:

Created by well funded, organized groups, nation-state actors, etc. Desire to compromise government and commercial entities, e.g. Flame: used for reconnaissance and information gathering of system.

Spyware and Adware:

Normally gets installed along with free software downloads. Spies on the end-user, attempts to redirect the user to specific sites. Main tasks: Behavioral surveillance and advertising with pop up ads Slows down the system.

Malware is short for malicious software, and refers to any software that is designed to cause harm to computer systems, networks, or users. Malware can take many forms, including:

1. Virus: A program that infects other software and replicates itself, spreading from one computer to another.
2. Worm: A program that replicates itself and spreads over a network, without the need for a host file.
3. Trojan: A program that appears to be legitimate but contains hidden malicious functionality.
4. Ransomware: A program that encrypts a user's files and demands payment in exchange for the decryption key.
5. Adware: Software that displays unwanted ads on a user's computer or device.
6. Spyware: Software that collects information about a user's computer usage and sends it to a third party without the user's knowledge or consent.
7. Rootkit: Software that provides an attacker with administrator-level access to a computer or network.
8. Backdoor: A program that allows unauthorized access to a computer system.

It’s important for individuals and organizations to be aware of the different types of malware and take steps to protect their systems, such as using antivirus software, keeping software and systems up-to-date, and being cautious when opening email attachments or downloading software from the internet.

Malware is a program designed to gain access to computer systems, normally for the benefit of some third party, without the user’s permission. Malware includes computer viruses, worms, Trojan horses, ransomware, spyware and other malicious programs. **Types of Malware:**

- **Viruses –** A Virus is a malicious executable code attached to another executable file. The virus spreads when an infected file is passed from system to system. Viruses can be harmless or they can modify or delete data. Opening a file can trigger a virus. Once a program virus is active, it will infect other programs on the computer.
- **Worms –** Worms replicate themselves on the system, attaching themselves to different files and looking for pathways between computers, such as computer network that shares common file storage areas. Worms usually slow down networks. A virus needs a host program to run but worms can run by themselves. After a worm affects a host, it is able to spread very quickly over the network.
- **Spyware –** Its purpose is to steal private information from a computer system for a third party. Spyware collects information and sends it to the hacker.
- **Trojan horse –** A Trojan horse is malware that carries out malicious operations under the appearance of a desired operation such as playing an online game. A Trojan horse varies from a virus because the Trojan binds itself to non-executable files, such as image files, audio files.
- **Logic Bombs –** A logic bomb is a malicious program that uses a trigger to activate the malicious code. The logic bomb remains non-functioning until that trigger event happens. Once triggered, a logic bomb implements a malicious code that causes harm to a computer. Cybersecurity specialists recently discovered logic bombs that attack and destroy the hardware components in a workstation or server including the cooling fans, hard drives, and power supplies. The logic bomb overdrives these devices until they overheat or fail.
- **Ransomware –** Ransomware grasps a computer system or the data it contains until the victim makes a payment. Ransomware encrypts data in the computer with a key which is unknown to the user. The user has to pay a ransom (price) to the criminals to retrieve data. Once the amount is paid the victim can resume using his/her system.
- **Backdoors –** A backdoor bypasses the usual authentication used to access a system. The purpose of the backdoor is to grant the cyber criminals future access to the system even if the organization fixes the original vulnerability used to attack the system.
- **Rootkits –** A rootkit modifies the OS to make a backdoor. Attackers then use the backdoor to access the computer distantly. Most rootkits take advantage of software vulnerabilities to modify system files.
- **Keyloggers –** Keylogger records everything the user types on his/her computer system to obtain passwords and other sensitive information and send them to the source of the keylogging program.

Advantages of Detecting and Removing Malware:

1. Improved Security: By detecting and removing malware, individuals and organizations can improve the security of their systems and reduce the risk of future infections.
2. Prevent Data Loss: Malware can cause data loss, and by removing it, individuals and organizations can protect their important files and information.
3. Protect Reputation: Malware can cause harm to a company's reputation, and by detecting and removing it, individuals and organizations can protect their image and brand.
4. Increased Productivity: Malware can slow down systems and make them less efficient, and by removing it, individuals and organizations can increase the productivity of their systems and employees.

Disadvantages of Detecting and Removing Malware:

1. Time-Consuming: The process of detecting and removing malware can be time-consuming and require specialized tools and expertise.
2. Cost: Antivirus software and other tools required to detect and remove malware can be expensive for individuals and organizations.
3. False Positives: Malware detection and removal tools can sometimes result in false positives, causing unnecessary alarm and inconvenience.
4. Difficulty: Malware is constantly evolving, and the process of detecting and removing it can be challenging and require specialized knowledge and expertise.
5. Risk of Data Loss: Some malware removal tools can cause unintended harm, resulting in data loss or system instability.

What is Ransomware?

Ransomware is a form of malicious software that prevents computer users from accessing their data by encrypting it. Cybercriminals use it to extort money from individuals or organizations whose data they have hacked, and they hold the data hostage until the ransom is paid.

If the cybercriminals do not pay the ransom within the specified time frame, the data may leak to the public or be permanently damaged. One of the most serious issues that businesses face is ransomware.

Businesses, individuals, and government organizations have all been victims of ransomware attacks since the mid-2000s, with the recovery of their systems costing large sums of money.

How does a computer get infected with ransomware?

One of the most commonly used tactics is phishing. Attackers spread malicious content using email, social media, advertisements, and website pop-ups, among other methods. Let's take some of these:

- **Email Phishing:** Cybercriminals use this approach to distribute ransomware all the time. Emails are carefully constructed to mislead the victim into clicking a link or opening an attachment. The malicious file that attacks the system is contained in the link or attachment, and when clicked, it will gain access to system files and data. When malware infects a computer, it encrypts the files and, in some circumstances, locks down the machine's owner or users. Other systems (computers and servers) connected to the network will be infected with more sophisticated ransomware.
- **Website Pop-ups:** When you click on malicious pop-ups on random websites, ransomware can infect your machine. Despite the fact that not all website pop-ups are malicious, hackers use them to extort money from their victims. Pop-ups from ransomware attackers often prompt you to update a program on your computer or make you believe that your system is infected with malware and that you need to click a link to remove it.
- **Remote Control Desktop:** Remote Control Desktop was designed to allow IT managers to access machines remotely for work purposes. Despite the fact that it was set up with good intentions, hackers have turned it into a money-making scheme. Port 3389 is used for desktop control. Since port 3389 is open on many systems, hackers can gain access to systems they identify as vulnerable. They will gain access by trying to log in as administrators using brute-force methods. Cyber thieves will have full access to the computer and will be able to encrypt any data as soon as they become an administrator. Some cybercriminals go even further, disabling endpoint protection or destroying Windows file backups.
- **Drive-By Downloads:** This method of compromising a user's machine occurs without the user's knowledge- ransomware attacks occur when a user visits a hacked website. The user does not need to click on anything before the virus spreads. Drive-by downloads on legal websites are commonly used by cybercriminals, especially if the website is susceptible. On the other hand, other cybercriminals create a website instead of breaking into one. When a visitor accesses an actual website that has been infected with malware, they will be redirected to another site that cybercriminals completely control. Once the user's PC is hacked, a ransom letter will appear requesting money for system unblocking and file decryption.

How to stop ransomware

- **Avoid Unverified Links:** If you want to be safe, this is important. Don't open emails from unknown senders or those you haven't subscribed to. Also, stay away from unknown websites.
- **Frequently Update Your Operating System and Software:** Keeping your operating system and software up to date can prevent ransomware. If you update to the latest security fixes, you will benefit from having them. This will result in cybercriminals having a harder time finding vulnerable software.
- **Make a System Backup:** If your data is lost or compromised, having a system backup can save you a lot of pain. Have it backed up both locally and in the cloud. This is a simple way to ensure that cybercriminals don't get over your personal

information. If your machine is infected with a ransomware virus, the backup will allow you to restore the system. Then, using your updated backup data, you can fix it. Backing up your data in the cloud adds an extra layer of security.

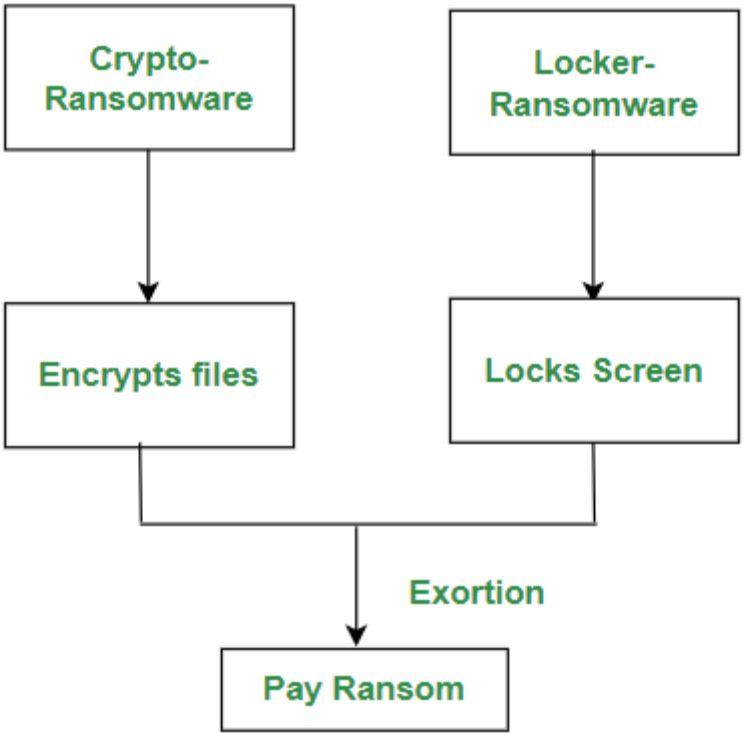
- **Restrict Access To Your Data:** This is accomplished by network isolation, which is important in the face of various cyber threats. Hackers are unable to gain easy access to data even when access is restricted. In the case of a ransomware virus attack, an isolating network protects the data.
- **Disable vulnerable plug-ins:** Hackers can easily damage your system by using plug-ins like Flash. They can use them to infect your machine and launch an attack. It exposes all your information which can be used to extort money from you. Keeping your plug-ins up to date is important to keep your system safe from virus attacks.
- **File Extensions:** From reputable sources, all documents/files must have the appropriate viewable file extensions. It is important to keep the system secure from downloading irrelevant documents from unknown sources.
- **In the Workplace, Ransomware Awareness:** Most ransomware virus attacks are caused by human errors. The answer is to ensure that workers are aware of the problem and are adequately trained to prevent and respond to it. Employees should be informed about the many hacking tips available. They should be aware that clicking on unfamiliar links or viewing harmful information can have serious consequences. All links and attachments should be double-checked and the source should be thoroughly checked before access. Furthermore, ransomware virus attacks can take many different forms. Phishing is only one of many types of attacks. Employees working from home must be connected to the public or open Wi-Fi. Hackers can easily gain access to these and launch attacks on your machine.
- **Create Strong Passwords:** Weak passwords are very easy to crack. When creating a password, don't include information that's easily available, such as your date of birth. If you use the same password for all your accounts, then hackers can gain access to your system. Finally, when creating passwords, avoid using easily accessible information. Some passwords contain information that can be easily obtained through the victim's social media accounts. These are vulnerable, and even a novice hacker will be able to detect them in no time. As a result, businesses and institutions must implement a strong password policy to keep hackers out.

Ransomware is a type of malware that denies access to data files using encryption until a ransom is paid. It comes under the category of cyber extortion. Ransomware does not intend to cause any damage to the computer's file system instead, it displays a ransom note on the victim's screen so that the victim can pay a certain amount of money to remove the restrictions and regain access to their computer, usually via a key. The malware creator will either supply a program that can decrypt the files, or will send an unlock code that decrypts the victim's data. But there is no guarantee that this will happen, even if the requested ransom is paid.

Types of Ransomware

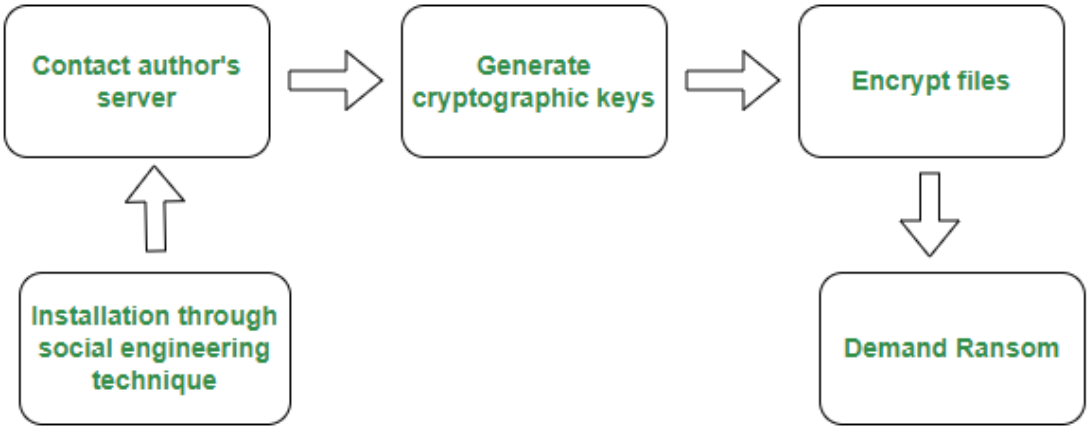
The two major types of ransomware are:

1. Crypto-Ransomware
2. Locker Ransomware



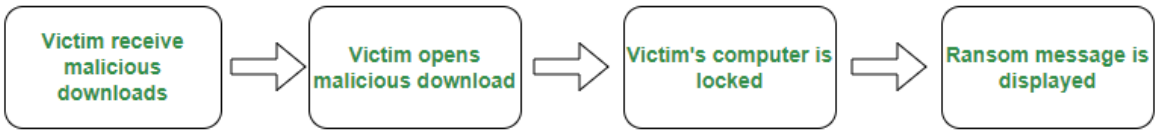
Types of Ransomware

Crypto Ransomware:
Crypto ransomware aims to encrypt sensitive files on the victim's computer. It does not block any basic computer function. This ransomware searches for important files on the local hard drive and external drives of the victim's system and starts encrypting them. Then, it will present a ransom note to the victim, showing a countdown timer and asking for payment. The attackers generate income by holding the valuable files hostage and demanding a ransom through anonymous methods such as Bitcoin to regain access to these files.



Crypto Ransomware process

Locker Ransomware:
Locker ransomware locks the victim out of their device and blocks the basic computer functions. Some parts of the keyboard may be locked and the mouse can be frozen allowing the victim only to respond to the attacker's demands. In this case, attackers demand ransom to unlock the device. The locked system only allows limited access, to interact with the attacker.



Locker Ransomware process

Other types of ransomware are:
1. Doxware: Doxware is ransomware that not only encrypts the files on the victim's computer but also steals the data from sensitive files. This ransomware extorts the victim by threatening to publish the stolen data online if the ransom is not paid. It may include private photos, emails, confidential information, etc.
2. Scareware: Scareware aims at convincing users to download useless software, damaging malware or ransomware which can hold users' data hostage and demand money. It uses social engineering to trick the users to install fake antivirus software.
3. Ransomware as a Service (RaaS): Ransomware as a Service is a business model between ransomware developers and affiliates to use developed ransomware tools to execute attacks. The affiliates earn a portion of each successful ransom payment.
The ways of encountering ransomware are:

1. Links or files are delivered through emails, messages, or other networks.
2. Downloaded onto the device by trojan downloader or exploit kits.

Examples of Ransomware Strains:

1. Cryptolocker
2. CryptoDefense
3. Bad Rabbit
4. Goldeneye
5. Zcryptor
6. Jigsaw
7. Petya

Prevention from Ransomware Infection:
Ransomware infection can be prevented by

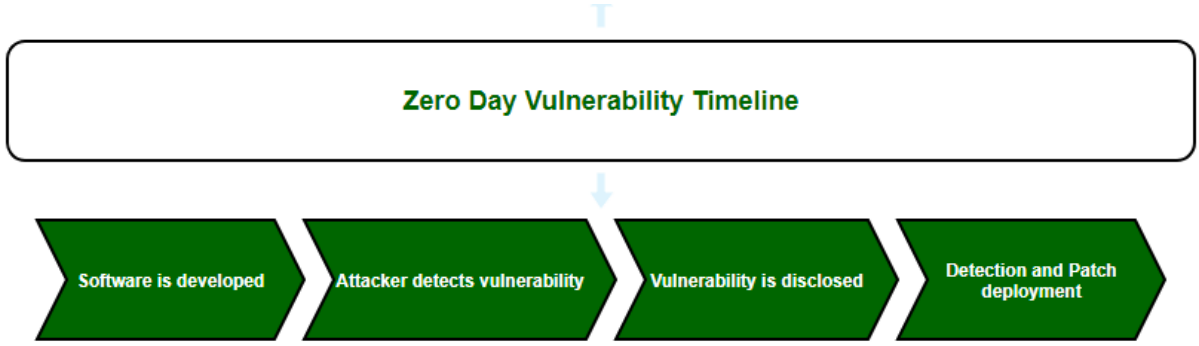
1. Not clicking on unsafe links.
2. Using security software.
3. Avoid the use of unknown USB sticks.
4. Not opening suspicious email attachments.
5. Downloading only from known sources.
6. Keeping the operating system and programs up to date

•

<u>Zero-day Exploit (Cyber Security Attack)</u>
In this IT era, majority of the cyberspaces are vulnerable to different kinds of attacks.

Zero-day exploit is a type of cyber security attack that occur on the same day the software, hardware or firmware flaw is detected by the manufacturer. As it's been zero days since the security flaw was last exploit, the attack is termed as zero-day exploit or zero-day attack. This kind of cyber-attacks are considered dangerous because the developer have not had the chance to fix the flaw yet. Zero-day exploit typically targets large organizations, government departments, firmware, hardware devices, IoT, users having access to valuable business data, etc.

Working of Zero-day Exploit:
A software is developed and released without knowing the fact that it has a security vulnerability. An attacker identifies or exploits this vulnerability before the developers identifies or fixes the same. While still the vulnerability is open and unpatched, exploiting the vulnerability, the hacker attacks and compromises the software which can lead to data theft, unauthorized access or crashing of the software itself. After the attacker attacks the target, the public or developer identifies the attack and tries to figure out the patch. The developer identifies the fix and releases the update to safe guard its new user.



Zero-day Exploit Detection:
Probability of detecting zero day exploit is rare or in other words, the attack leaves no opportunity for detection. But there are a few ways to identify the existing known vulnerabilities.

1. **Signature Based –** In this method, the occurrence pattern of known vulnerability can be detected with the help of pattern matching. Even though this method cannot detect the malware code used for zero-day exploit, it is capable of detecting known attacks like SQL injection that may lead to zero-day vulnerability. While a developer may not be able to detect zero-day attack, the system firewall may be able to detect and protect against few known specific attack types such as XSS , SQL injection, etc.
2. **Statistical Techniques –** By monitoring the normal activity, this technique learns the normal behavior of the network. When the system identifies any deviation from normal profile it will detect a probability of vulnerability.
3. **Behavior Based –** The implementation of behavior based detection typically depends on a 'honeypot'. A honeypot is a security mechanism that is developed to detect the presence of hackers or hacking attempts.
4. **Hybrid Techniques –** This hybrid technique use the advantage of statistical, behavioral and traditional signature based defense mechanism. They are comparatively more effective as the weaknesses of any single detection technique will not break the security.

Zero-day Exploit Prevention : As zero-day exploits cannot be easily discovered, prevention of the zero-day exploit becomes difficult. There is hardly any ways to protect against zero-day exploit as we don't have any idea about its occurrence well in advance. We can reduce the level of risk opting any of the following strategies:

- Implementation of IP security protocol (IPSec).
- Usage of virtual local area networks.
- Deployment of intrusion detection system (IDS) or intrusion prevention system (IPS).
- Usage of network access control protocols.
- Usage of security schemes such as Wi-Fi Protected Access 2.
- Keeping all systems up to date.
- Performing periodic vulnerability scanning.

Example Cases of Zero-day Exploit :

- **CVE-2016-4117 –** This zero-day attack exploited one of the previously undiscovered flaws in Adobe Flash Player.

- **CVE-2016-0167 –** This is a privilege escalation attack targeting win32k Windows Graphics subsystem Microsoft Windows.
- **CVE-2017-0199 –** This zero-day attack exploited one of the previously undisclosed vulnerability in Microsoft Office RTF documents.
- **Stuxnet worm –** This zero-day exploit targeted supervisory control and data acquisition (SCADA) systems.

What is zero-click malware, and how do zero-click attacks work?

In recent years, zero-click attacks have occasionally made their way into the spotlight. As the name suggests, zero-click attacks require no action from the victim – meaning that even the most advanced users can fall prey to serious cyber hacks and spyware tools.

Zero-click attacks are typically highly targeted and use sophisticated tactics. They can have devastating consequences without the victim even knowing that something is wrong in the background. The terms 'zero-click attacks' and 'zero-click exploits' are often used interchangeably. They are sometimes also called interaction-less or fully remote attacks.

What is zero-click malware?

Traditionally, spying software relies on convincing the targeted person to click on a compromised link or file to install itself on their phone, tablet, or computer. However, with a zero-click attack, the software can be installed on a device without the victim clicking on any link. As a result, zero-click malware or no-click malware is much more dangerous.

The reduced interaction involved in zero-click attacks means fewer traces of any malicious activity. This – plus the fact that vulnerabilities which cybercriminals can exploit for zero-click attacks are quite rare – make them especially prized by attackers.

Even basic zero-click attacks leave little trace, which means detecting them is extremely difficult. Additionally, the same features which make software more secure can often make zero-click attacks harder to detect. Zero-click hacks have been around for years, and the issue has become more widespread with the booming use of smartphones that store a wealth of personal data. As individuals and organizations become increasingly reliant on mobile devices, the need to stay informed about zero-click vulnerabilities has never been greater.

How does a zero-click attack work?

Typically, remote infection of a target's mobile device requires some form of social engineering, with the user clicking on a malicious link or installing a malicious app to provide the attacker with an entry point. This is not the case with zero-click attacks, which bypass the need for social engineering entirely.

A zero-click hack exploits flaws in your device, making use of a data verification loophole to work its way into your system. Most software uses data verification processes to keep cyber breaches at bay. However, there are persistent zero-day vulnerabilities that are not yet patched, presenting potentially lucrative targets for cybercriminals. Sophisticated hackers can exploit these zero-day vulnerabilities to execute cyber-attacks, which can be implemented with no action on your part.

Often, zero-click attacks target apps that provide messaging or voice calling because these services are designed to receive and interpret data from untrusted sources. Attackers generally use specially formed data, such as a hidden text message or image file, to inject code that compromises the device.

A hypothetical zero-click attack might work like this:

- Cybercriminals identify a vulnerability in a mail or messaging app.
- They exploit the vulnerability by sending a carefully crafted message to the target.
- The vulnerability allows malicious actors to infect the device remotely via emails that consume extensive memory.
- The hacker's email, message, or call won't necessarily remain on the device.
- As a result of the attack, cybercriminals can read, edit, leak, or delete messages.

The hack can be a series of network packets, authentication requests, text messages, MMS, voicemail, video conferencing sessions, phone calls, or messages sent over Skype, Telegram, WhatsApp, etc. All of these can exploit a vulnerability in the code of an application tasked with processing the data.

The fact that messaging apps allow people to be identified with their phone numbers, which are easily locatable, means that they can be an obvious target for both political entities and commercial hacking operations.

The specifics of each zero-click attack will vary depending on which vulnerability is being exploited. A key trait of zero-click hacks is their ability not to leave behind traces, making them very difficult to detect. This means that is not easy to identify who is using them and for what purpose. However, it is reported that intelligence agencies worldwide use them to intercept messages from and monitor the whereabouts of suspected criminals and terrorists.

Examples of zero-click malware

A zero-click vulnerability can affect various devices, from Apple to Android. High profile examples of zero-click exploits include:

Apple zero-click, forced entry, 2021:
In 2021, a Bahraini human rights activist had their iPhone hacked by powerful spyware sold to nation-states. The hack, uncovered by researchers at Citizen Lab, had defeated security protections put in place by Apple to withstand covert compromises.

Citizen Lab is an internet watchdog based at the University of Toronto. They analyzed the activist’s iPhone 12 Pro and found that it had been hacked via a zero-click attack. The zero-click attack took advantage of a previously unknown security vulnerability in Apple’s iMessage, which was exploited to push Pegasus spyware, developed by the Israeli firm NGO Group, to the activist’s phone.

The hack attracted significant news coverage, mainly because it exploited the latest iPhone software at the time, both iOS 14.4 and later iOS 14.6, which Apple released in May 2021. The hack overcame a security software feature built into all versions of iOS 14, called BlastDoor, which was intended to prevent this kind of device hacks by filtering malicious

data sent over iMessage. Because of its ability to overcome BlastDoor, this exploit was dubbed ForcedEntry. In response, Apple upgraded its security defenses with iOS 15.

WhatsApp breach, 2019:
This infamous breach was triggered by a missed call, which exploited a flaw in the source code framework of WhatsApp. A zero-day exploit – i.e., a previously unknown and unpatched cyber vulnerability – allowed the attacker to load spyware in the data exchanged between two devices due to the missed call. Once loaded, the spyware enabled itself as a background resource, deep within the device's software framework.

Jeff Bezos, 2018:
In 2018, Crown Prince Mohammed bin Salman of Saudi Arabia allegedly sent Amazon CEO Jeff Bezos a WhatsApp message with a video promoting Saudi Arabia's telecom market. It was reported that there was a piece of code within the video file that enabled the sender to extract information from Bezos's iPhone over several months. This resulted in the capture of text messages, instant messages, and emails, and possibly even eavesdropped recordings taken with the phone's microphones.

Project Raven, 2016:
Project Raven refers to the UAE's offensive cyber operations unit, which comprises Emirati security officials and former US intelligence operators working as contractors. Reportedly, they used a tool known as Karma to take advantage of a flaw in iMessage. Karma used specially crafted text messages to hack into the iPhones of activists, diplomats, and rival foreign leaders to obtain photos, emails, text messages, and location information.

How to protect yourself from zero-click exploits

Because zero-click attacks are based on no interaction from the victim, it follows that there isn't much you can do to protect yourself. While that is a daunting thought, it's important to remember that, in general, these attacks tend to be targeted at specific victims for espionage purposes or perhaps monetary gain.

That said, practicing basic cyber hygiene will help to maximize your online safety. Sensible precautions you can take include:

- Keep your operating system, firmware, and apps on all your devices up to date as prompted.
- Only download apps from official stores.
- Delete any apps you no longer use.
- Avoid 'jailbreaking' or 'rooting' your phone since doing so removes protection provided by Apple and Google.
- Use your device password protection.
- Use strong authentication to access accounts, especially critical networks.
- Use strong passwords – i.e., long and unique passwords.
- Regularly backup systems. Systems can be restored in cases of ransomware, and having a current backup of all data speeds the recovery process.
- Enable pop-up blockers or prevent pop-ups from appearing by adjusting your browser settings. Scammers routinely use pop-ups to spread malware.

Leagal perspective in cyber crime

Overview of cyber crimes and cyber law

What is cyber crime

Any criminal activity that involves a computer, networked device, or any other related device can be considered a cyber crime. There are some instances when cyber crimes are carried out with the intention of generating profit for the cybercriminals, whereas other times a cyber crime is carried out directly to damage or disable the computer or device. It is also possible that others use computers or networks to spread malware, illegal information, images, or any other kind of material.

As a result of cyber crime, many types of profit-driven criminal activities can be perpetrated, such as ransomware attacks, email and internet fraud, identity theft, and frauds involving financial accounts, credit cards or any other payment card. The theft and resale of personal and corporate data could be the goal of cybercriminals.

In India, cyber crimes are covered by the Information Technology Act, 2000 and the Indian Penal Code, 1860. It is the Information Technology Act, 2000, which deals with issues related to cyber crimes and electronic commerce. However, in the year 2008, the Act was amended and outlined the definition and punishment of cyber crime. Several amendments to the Indian Penal Code 1860 and the Reserve Bank of India Act were also made.

Types of cyber crimes

The following are considered to be types of cyber-crimes:

Child pornography or child sexually abusive material (CSAM):

In its simplest sense, child sexual abuse materials (CSAMs) include any material containing sexual images in any form, wherein both the child being exploited or abused may be seen. There is a provision in Section 67(B) of the Information Technology Act which states that the publication or transmission of material depicting children in sexually explicit acts in an electronic form is punishable.

Cyberbullying:

A cyberbully is someone who harasses or bullies others using electronic devices like computers, mobile phones, laptops, etc. Cyberbullying refers to bullying conducted through the use of digital technology. The use of social media, messaging platforms, gaming

platforms, and mobile devices may be involved. Oftentimes, this involves repeated behaviour that is intended to scare, anger, or shame those being targeted.

Cyberstalking:

Cyberstalking is the act of harassing or stalking another person online using the internet and other technologies. Cyberstalking is done through texts, emails, social media posts, and other forms and is often persistent, methodical, and deliberate.

Cyber grooming:

The phenomenon of cyber grooming involves a person building a relationship with a teenager and having a strategy of luring, teasing, or even putting pressure on them to perform a sexual act.

Online job fraud:

An online job fraud scheme involves misleading people who require a job by promising them a better job with higher wages while giving them false hope. On March 21, 2022, the Reserve Bank of India (RBI) alerted people not to fall prey to job scams. By this, the RBI has explained the way in which online job fraud is perpetrated, as well as precautions the common man should take when applying for any job opportunity, whether in India or abroad.

Online sextortion:

The act of online sextortion occurs when the cybercriminal threatens any individual to publish sensitive and private material on an electronic medium. These criminals threaten in order to get a sexual image, sexual favour, or money from such individuals.

Phishing:

Fraud involving phishing is when an email appears to be from a legitimate source but contains a malicious attachment that is designed to steal personal information from the user such as their ID, IPIN, Card number, expiration date, CVV, etc. and then selling the information on the dark web.

Vishing:

In vishing, victims' confidential information is stolen by using their phones. Cybercriminals use sophisticated social engineering tactics to get victims to divulge private information and access personal accounts. In the same way as phishing and smishing, vishing convincingly fools victims into thinking that they are being polite by responding to the call. Callers can

often pretend that they are from the government, tax department, police department, or victim's bank..

Smishing:

As the name suggests, smishing is a fraud that uses text messages via mobile phones to trick its victims into calling a fake phone number, visiting a fraudulent website or downloading malicious software that resides on the victim's computer.

Credit card fraud or debit card fraud:

In credit card (or debit card) fraud, unauthorized purchases or withdrawals from another's card are made to gain access to their funds. When unauthorized purchases or withdrawals of cash are made from a customer's account, they are considered credit/debit card fraud. Fraudulent activity occurs when a criminal gains access to the cardholder's debit/credit number, or personal identification number (PIN). Your information can be obtained by unscrupulous employees or hackers.

Impersonation and identity theft:

A person is impersonated or exposed to identity theft when they make fraudulent use of an electronic signature, a password, or any other unique identifier on another person's behalf.

Prevention of cyber crimes

As per the recommendations of the International Maritime Organization (IMO), the cyber-attack risk must be approached using the following framework:

- The first step is to define the roles and responsibilities of the personnel responsible for cyber risk management.
- The second step is to identify the systems, assets, data, or capabilities that will put the operation at stake if disrupted.
- To protect against a potential cyber event and to maintain continuity of operations, it is important to implement risk-control processes and contingency plans.
- It is also important to develop and implement measures to detect a cyber-attack as quickly as possible.
- Preparation and implementation of plans to restore critical systems for continued operations by providing resilience.
- Finally, identify and implement measures to be taken to backup and restore any affected systems.

The following can be the strategies can be used to prevent cyber crime:

Analyze your risk exposure:

In order to adequately prepare for a cyber attack, you must assess the threat and give due consideration. Companies should consider the following:

- They should consider all areas where they are susceptible to cyberattacks and any operational vulnerabilities resulting from them.
- A vulnerability assessment of all systems is necessary to identify those that are critical to the business, to understand the potential exposures each has, and to assess the impact of any cyber-attack on business continuity.
- IT systems and operational technology systems should be checked by businesses.

Preventive measures:

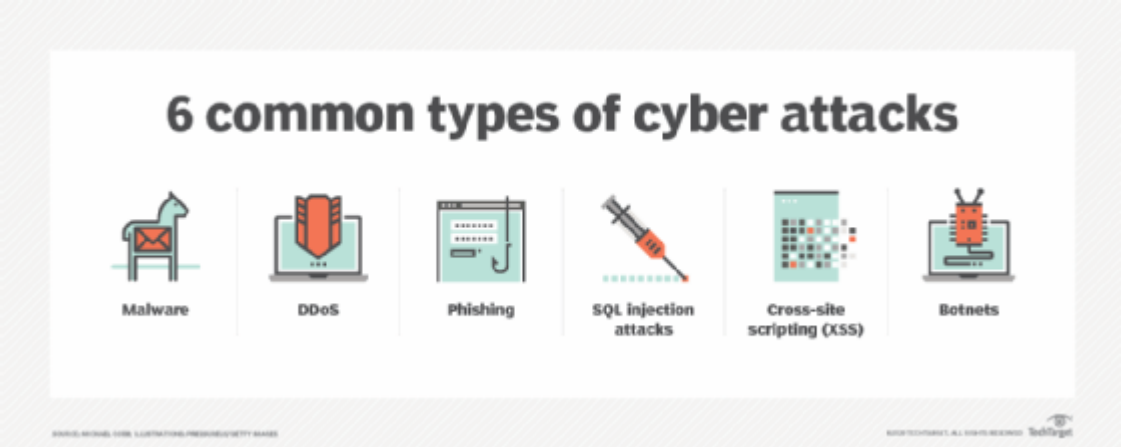
It is recommended that businesses adopt national or international technical standards that provide a high level of protection. These general prevention measures are recommended for companies that currently lack the necessary technical or financial capabilities. The following is the list of preventive measures:

- Applying multiple layers of defence, beginning with physical security, followed by management policies and procedures, firewalls and network architecture, computer policies, account management, security updates and finally antivirus applications.
- Implementing a principle of least privilege, which restricts information and access to only those set of people who needs to know that particular information.
- Implementing network-hardening measures, assuring patch management is sufficient and is proactively reviewed.
- Securing critical systems by utilizing technology such as protocol-aware filtering and segregation.
- Ensuring that removable devices are encrypted and that any USB used with any other device is tested for viruses.
- Furthermore, in order to prevent the negative impact of a cyberattack from further escalating and restoring business operations, it is important to develop business continuity plans, identify key personnel, and implement processes.
- Additionally, organising frequent training and awareness sessions for all employees can also help.
- Compliance audits of third-party service providers will also be beneficial.

Cyber crime laws in India

In terms of cybersecurity, there are five main types of laws that must be followed. Cyber laws are becoming increasingly important in countries such as India which have extremely extensive internet use. There are strict laws that govern the use of cyberspace and supervise

the use of information, software, electronic commerce, and financial transactions in the digital environment. India's cyber laws have helped to enable electronic commerce and electronic governance to flourish in India by safeguarding maximum connectivity and minimizing security concerns. This has also made digital media accessible in a wider range of applications and enhanced its scope and effectiveness.



Who does the Information Technology Amendment Act apply to?

The Information Technology Amendment Act is applicable to any person, company or organization that uses computer systems, computer networks or other information technology in India.

This includes but is not limited to the following:

- web hosting service providers
- internet service providers
- network service providers
- telecom service providers

This includes foreign companies and organizations with a presence in India, as well as Indian companies and organizations with operations outside of India.

Indian Penal Code, 1860 (IPC):

If the IT Act is not sufficient to cover specific cyber crimes, law enforcement agencies can apply the following IPC sections:

- Section 292: The purpose of this section was to address the sale of obscene materials, however, in this digital age, it has evolved to deal with various cyber crimes as well. A manner in which obscene material or sexually explicit acts or exploits of children are published or transmitted electronically is also governed by this provision. The penalty for such acts is imprisonment and fines up to 2 years and Rs. 2000, respectively. The punishment for any of the above crimes may be up to five years of imprisonment and a fine of up to Rs. 5000 for repeat (second-time) offenders.
- Section 354C: In this provision, cyber crime is defined as taking or publishing pictures of private parts or actions of a woman without her consent. In this section, voyeurism is discussed exclusively since it includes watching a woman's sexual actions as a crime. In the absence of the essential elements of this section, Section 292 of the IPC and Section 66E of the IT Act are broad enough to include offences of an equivalent nature. Depending on the offence, first-time offenders can face up to 3 years in prison, and second-time offenders can serve up to 7 years in prison.
- Section 354D: Stalking, including physical and cyberstalking, is described and punished in this chapter. The tracking of a woman through electronic means, the internet, or email or the attempt to contact her despite her disinterest amounts to cyber-stalking. This offence is punished by imprisonment of up to 3 years for the first offence and up to 5 years for the second offence, along with a fine in both cases.

A victim in the case *Kalandi Charan Lenka v. the State of Odisha(2017)* has received a series of obscene messages from an unknown number that has damaged her reputation. The accused also sent emails to the victim and created a fake account on Facebook containing morphed images of her. The High Court, therefore, found the accused prima facie guilty of cyberstalking on various charges under the IT Act and Section 354D of IPC.

- Section 379: The punishment involved under this section, for theft, can be up to three years in addition to the fine. The IPC Section comes into play in part because many cyber crimes involve hijacked electronic devices, stolen data, or stolen computers.
- Section 420: This section talks about cheating and dishonestly inducing delivery of property. Seven-year imprisonment in addition to a fine is imposed under this section on cybercriminals doing crimes like creating fake websites and cyber frauds. In this section of the IPC, crimes related to password theft for fraud or the creation of fraudulent websites are involved.

- Section 463: This section involves falsifying documents or records electronically. Spoofing emails is punishable by up to 7 years in prison and/or a fine under this section.
- Section 465: This provision typically deals with the punishment for forgery. Under this section, offences such as the spoofing of email and the preparation of false documents in cyberspace are dealt with and punished with imprisonment ranging up to two years, or both. In *Anil Kumar Srivastava v. Addl Director, MHFW (2005)*, the petitioner had forged signed the signature of the AD and had then filed a case that made false allegations against the same individual. Due to the fact that the petitioner also attempted to pass it off as a genuine document, the Court held that the petitioner was liable under Sections 465 and 471 of the IPC.
- Section 468: Fraud committed with the intention of cheating may result in a seven-year prison sentence and a fine. This section also punishes email spoofing.

Furthermore, there are many more sections of the IT Act and the Indian Penal Code, which pertain to cyber crimes, in addition to the laws listed above.

Even though there are laws against cyber crime in place, the rate of cyber crime is still rising drastically. It has been reported that cyber crime in India increased by 11.8% in the year 2020, which accounted for reporting around only 50,000 cases. Cyber crime is one of the toughest crimes for the Police to solve due to many challenges they face including underreporting, the jurisdiction of crime, public unawareness and the increasing costs of investigation due to technology.

Certain offences may end up being bailable under the IPC but not under the IT Act and vice versa or maybe compoundable under the IPC but not under the IT Act and vice versa due to the overlap between the provisions of the IPC and the IT Act. For example, if the conduct involves hacking or data theft, offences under sections 43 and 66 of the IT Act are bailable and compoundable, whereas offences under Section 378 of the IPC are not bailable and offences under Section 425 of the IPC are not compoundable. Additionally, if the offence was the receipt of stolen property, the offence under section 66B of the IT Act was bailable while the offence under Section 411 of the IPC was not. In the same manner, in respect of the offence of identity theft and cheating by personation, the offences are compoundable and bailable under sections 66C and 66D of the IT Act, whereas the offences under Sections 463, 465, and 468 of the IPC are not compoundable and the offences under sections 468 and 420 of the IPC are not bailable.

In *Gagan Harsh Sharma v. The State of Maharashtra (2018)*, the Bombay High Court addressed the issue of non-bailable and non-compoundable offences under sections 408 and 420 of the IPC in conflict with those under Sections 43, 65, and 66 of the IT Act that is bailable and compoundable.

Information Technology Rules (IT Rules):

There are several aspects of the collection, transmission, and processing of data that are covered by the IT Rules, including the following:

- The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011: According to these rules, entities holding individuals' sensitive personal information must maintain certain security standards that are specified.
- The Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021: To maintain the safety online of users' data, these rules govern the role of intermediaries, including social media intermediaries, to prevent the transmission of harmful content on the internet.
- The Information Technology (Guidelines for Cyber Cafe) Rules, 2011: According to these guidelines, cybercafés must register with an appropriate agency and maintain a record of users' identities and their internet usage.
- The Information Technology (Electronic Service Delivery) Rules, 2011: Basically, these regulations give the government the authority to specify the delivery of certain services, such as applications, certificates, and licenses, by electronic means.
- Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (the CERT-In Rules): There are several ways in which the CERT-In rules provide for the working of CERT-In. In accordance with rule 12 of the CERT-In rules, a 24-hour Incident response helpdesk must be operational at all times. Individuals, organisations and companies can report cybersecurity incidents to Cert-In if they are experiencing a cybersecurity Incident. The Rules provide an Annexure listing certain Incidents that must be reported to Cert-In immediately.

Another requirement under Rule 12 is that service providers, intermediaries, data centres, and corporate bodies inform CERT-In within a reasonable timeframe of cybersecurity incidents. As a result of the Cert-In website, Cybersecurity Incidents can be reported in various formats and methods, as well as information on vulnerability reporting, and incident response procedures. In addition to reporting cybersecurity incidents to CERT-In in accordance with its rules, Rule 3(1)(I) of the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021 also requires that all intermediaries shall disclose information about cybersecurity incidents to CERT-In.

Information Technology Amendment Act 2008 (IT Act 2008)

The Information Technology Amendment Act 2008 (IT Act 2008) is a substantial addition to India's Information Technology Act 2000.

The Information Technology Amendment Act was passed by the Indian Parliament in October 2008 and came into force a year later. The act is administered by the Indian Computer Emergency Response Team (CERT-In) and corresponds to the Indian Penal Code.

The Information Technology Amendment Act has been widely hailed as a progressive step forward in protecting India's cyber infrastructure and citizens.

It is one of the most comprehensive pieces of legislation addressing IT-related issues and sets a strong precedent for other countries working to update their own laws.

Why was the Information Technology Amendment Act created?

The original version of the act was developed to promote the IT industry, regulate e-commerce, facilitate e-governance and prevent cybercrime.

However, it also sought to foster security practices within India that would serve the country in a global context.

In addition, the Information Technology Amendment Act established the office of the Cyber Appellate Tribunal to hear appeals from any person aggrieved by an order made under the act.

What does the Information Technology Amendment Act cover?

The Information Technology Amendment Act 2008 has nine chapters and 117 sections and covers a wide range of topics related to IT, cybercrime and data protection.

The act includes provisions for the following

- tightening cybersecurity measures
- establishing a legal framework for digital signatures
- recognizing and regulating intermediaries
- regulating interception, monitoring and decryption of electronic records
- cyber forensics
- cyberterrorism

Amendments to the act have been created to address issues that the original bill failed to cover and to accommodate further development of IT and related security concerns since the original law was passed.

How has the Information Technology Amendment Act been updated?

Changes to the amendment over the years have included the following:

- redefining terms such as *communication devices* to reflect current use;
- validating electronic signatures and contracts;
- making the owner of a given IP address responsible for content accessed or distributed through it; and
- making corporations responsible for implementing effective data security practices and liable for data breaches.

In recent years, the IT Act has also been updated to include provisions for the regulation of intermediaries, penalties for cybercrime and restrictions on certain types of speech.

These changes included expanding the definition of *cybercrime* and adding new penalties for offenses such as identity theft, publishing private images without consent, cheating by impersonation, and sending offensive messages or those containing sexually explicit acts through electronic means.

What are the penalties for violating the Information Technology Amendment Act?

Penalties for violating the Information Technology Amendment Act can range from a fine of 1 lakh rupees (approximately $1,250) to imprisonment for up to three years.

More serious offenses can result in a person being liable to pay damages up to 5 lakh rupees (approximately $6,300) and include imprisonment of up to seven years.

Cyberterrorism offenses are punishable by imprisonment of up to 10 years.

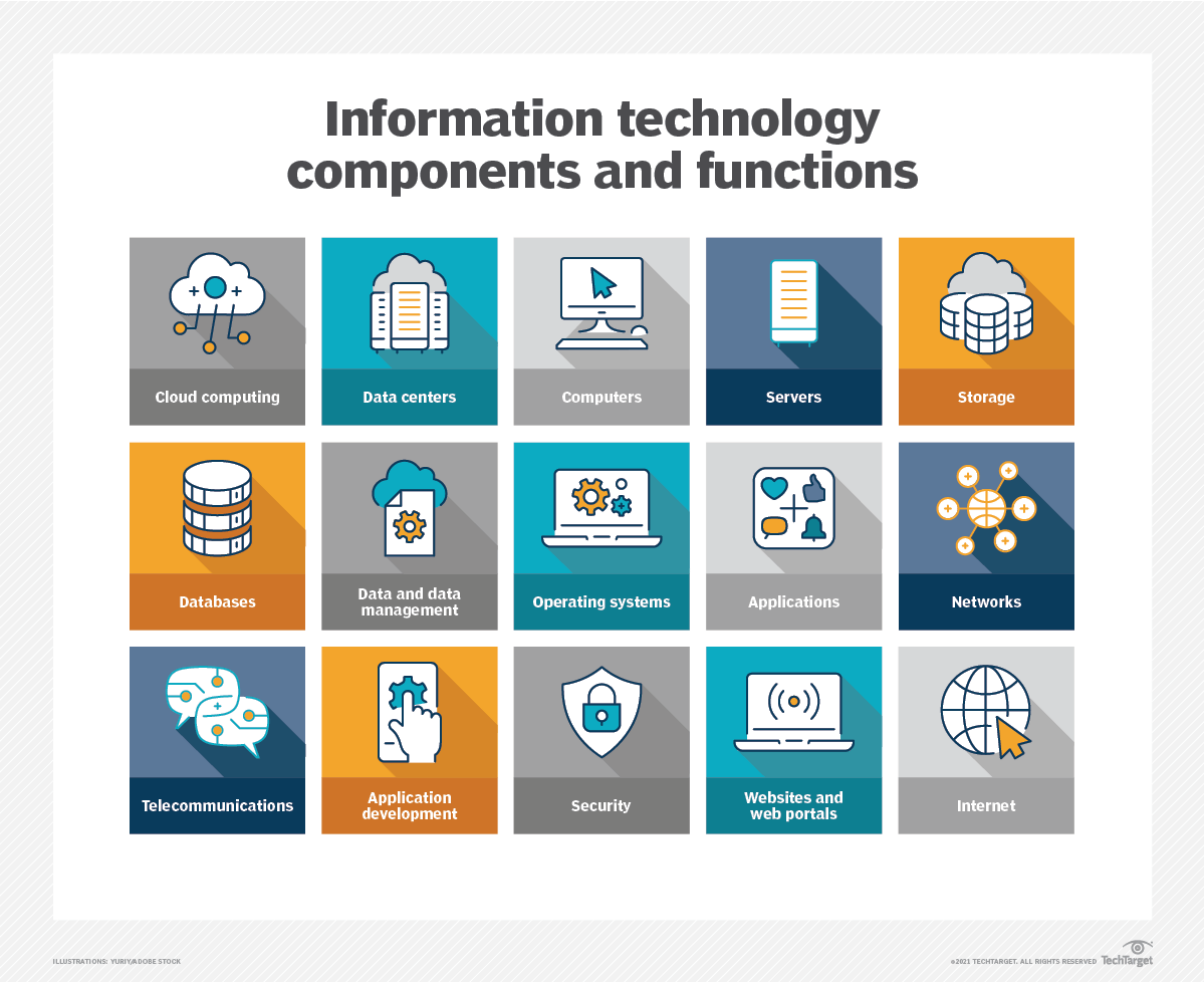
In addition to these penalties, the court can also order the offender to pay compensation to the victim of the offense.

Challenges with the Information Technology Amendment Act

The amendment has been criticized for decreasing the penalties for some cybercrimes and for lacking sufficient safeguards to protect the civil rights of individuals.

Subsection 69, for example, authorizes the Indian government to intercept, monitor, decrypt and block data at its discretion.

According to Pavan Duggal, a cyber law consultant and advocate at the Supreme Court of India: "The Act has provided the Indian government with the power of surveillance, monitoring and blocking data traffic. The new powers under the amendment act tend to give Indian government a texture and color of being a surveillance state."



Still, the IT Act has been instrumental in developing a comprehensive legal framework for IT in India.

It has been successful in establishing procedures for electronic governance and the prevention of cybercrime.

The act will likely continue to be amended as needed to reflect the ever-changing landscape of IT.

Cyber Crime and Offences

Cyber offences are the illegitimate actions, which are carried out in a classy manner where either the computer is the tool or target or both.

Cyber-crime usually includes the following −

- Unauthorized access of the computers
- Data diddling
- Virus/worms attack
- Theft of computer system
- Hacking
- Denial of attacks
- Logic bombs
- Trojan attacks
- Internet time theft
- Web jacking
- Email bombing
- Salami attacks
- Physically damaging computer system.

The offences included in the I.T. Act 2000 are as follows −

- Tampering with the computer source documents.
- Hacking with computer system.
- Publishing of information which is obscene in electronic form.
- Power of Controller to give directions.
- Directions of Controller to a subscriber to extend facilities to decrypt information.
- Protected system.
- Penalty for misrepresentation.
- Penalty for breach of confidentiality and privacy.
- Penalty for publishing Digital Signature Certificate false in certain particulars.
- Publication for fraudulent purpose.
- Act to apply for offence or contravention committed outside India Confiscation.
- Penalties or confiscation not to interfere with other punishments.
- Power to investigate offences.

Example

Offences Under The It Act 2000

Section 65. Tampering with computer source documents

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the being time in force, shall be punishable with imprisonment up to three year, or with fine which may extend up to two lakh rupees, or with both.

Explanation − For the purpose of this section "computer source code" means the listing of programs, computer commands, design and layout and program analysis of computer resource in any form.

Object − The object of the section is to protect the "intellectual property" invested in the computer. It is an attempt to protect the computer source documents (codes) beyond what is available under the Copyright Law

Section	Offence	Punishment	Bailability and Congizability
65	Tampering with Computer Source Code	Imprisonment up to 3 years or fine up to Rs 2 lakhs	Offence is Bailable, Cognizable and triable by Court of JMFC.
66	Computer Related Offences	Imprisonment up to 3 years or fine up to Rs 5 lakhs	Offence is Bailable, Cognizable and
66-A	Sending offensive messages through Communication service, etc...	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable and triable by Court of JMFC
66-B	Dishonestly receiving stolen computer resource or communication device	Imprisonment up to 3 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-C	Identity Theft	Imprisonment of either description up to 3 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-D	Cheating by Personation by using computer resource	Imprisonment of either description up to 3 years and /or fine up to Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-E	Violation of Privacy	Imprisonment up to 3 years and /or fine up to Rs. 2 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-F	Cyber Terrorism	Imprisonment extend to imprisonment for Life	Offence is Non-Bailable, Cognizable and triable by Court of Sessions
67	Publishing or transmitting obscene material in electronic form	On first Conviction, imprisonment up to 3 years and/or fine up to Rs. 5 lakh On Subsequent Conviction	Offence is Bailable, Cognizable and triable by Court of JMFC

		imprisonment up to 5 years and/or fine up to Rs. 10 lakh	
67-A	Publishing or transmitting of material containing sexually explicit act, etc... in electronic form	On first Conviction imprisonment up to 5 years and/or fine up to Rs. 10 lakh On Subsequent Conviction imprisonment up to 7 years and/or fine up to Rs. 10 lakh	Offence is Non-Bailable, Cognizable and triable by Court of JMFC
67-B	Publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form	On first Conviction imprisonment of either description up to 5 years and/or fine up to Rs. 10 lakh On Subsequent Conviction imprisonment of either description up to 7 years and/or fine up to Rs. 10 lakh	Offence is Non Bailable, Cognizable and triable by Court of JMFC
67-C	Intermediary intentionally or knowingly contravening the directions about Preservation and retention of information	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable.
68	Failure to comply with the directions given by Controller	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.
69	Failure to assist the agency referred to in sub section (3) in regard interception or monitoring or decryption of any information through any computer resource	Imprisonment up to 7 years and fine	Offence is Non-Bailable, Cognizable.
69-A	Failure of the intermediary to comply with the direction issued for blocking for public access of any information through any computer resource	Imprisonment up to 7 years and fine	Offence is Non-Bailable, Cognizable.
69-B	Intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) in regard monitor and collect traffic data or information through any computer resource for cybersecurity	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable.

70	Any person who secures access or attempts to secure access to the protected system in contravention of provision of Sec. 70	Imprisonment of either description up to 10 years and fine	Offence is Non-Bailable, Cognizable.
70-B	Indian Computer Emergency Response Team to serve as national agency for incident response. Any service provider, intermediaries, data centres, etc., who fails to prove the information called for or comply with the direction issued by the ICERT.	Imprisonment up to 1 year and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable
71	Misrepresentation to the Controller to the Certifying Authority	Imprisonment up to 2 years and/ or fine up to Rs. 1 lakh.	Offence is Bailable, Non-Cognizable.
72	Breach of Confidentiality and privacy	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh.	Offence is Bailable, Non-Cognizable.
72-A	Disclosure of information in breach of lawful contract	Imprisonment up to 3 years and/or fine up to Rs. 5 lakh.	Offence is Cognizable, Bailable
73	Publishing electronic Signature Certificate false in certain particulars	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.
74	Publication for fraudulent purpose	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.

Essential ingredients of the section

knowingly or intentionally concealing

knowingly or intentionally destroying

knowingly or intentionally altering

knowingly or intentionally causing others to conceal

knowingly or intentionally causing another to destroy

knowingly or intentionally causing another to alter.

This section extends towards the Copyright Act and helps the companies to protect their source code of their programs.

Penalties − Section 65 is tried by any magistrate.

This is cognizable and non-bailable offence.

Penalties − Imprisonment up to 3 years and / or

Fine − Two lakh rupees.

The following table shows the offence and penalties against all the mentioned sections of the I.T. Act −

Compounding of Offences

As per Section 77-A of the I. T. Act, any Court of competent jurisdiction may compound offences, other than offences for which the punishment for life or imprisonment for a term exceeding three years has been provided under the Act.

No offence shall be compounded if −

- *The accused is, by reason of his previous conviction, is liable to either enhanced punishment or to the punishment of different kind; OR*
- *Offence affects the socio economic conditions of the country; OR*
- *Offence has been committed against a child below the age of 18 years; OR*
- *Offence has been committed against a woman.*

The person alleged of an offence under this Act may file an application for compounding in the Court. The offence will then be pending for trial and the provisions of Sections 265-B and 265-C of Cr. P.C. shall apply.

Companies Act, 2013:

A majority of the corporate stakeholders consider the Companies Act of 2013 to be the most pertinent legal obligation to properly manage daily operations. This Act enshrines in law all the techno-legal requirements that need to be met, implementing the law as a challenge to the companies that are not compliant. As part of the Companies Act 2013, the SFIO (Serious Fraud Investigation Office) is entrusted with powers to investigate and prosecute serious frauds committed by Indian companies and their directors.

As a result of the Companies Inspection, Investment, and Inquiry Rules, 2014 notification, the SFIOs have become even more proactive and serious in regard to this. By ensuring proper coverage of all the regulatory compliances, the legislature ensured that every aspect of cyber forensics, e-discovery, and cybersecurity diligence is adequately covered. Moreover, the Companies (Management and Administration) Rules, 2014 prescribe a strict set of guidelines that confirm the cybersecurity obligations and responsibilities of corporate directors and senior management.

Cybersecurity Framework (NCFS):

As the most credible global certification body, the National Institute of Standards and Technology (NIST) has approved the Cybersecurity Framework (NCFS) as a framework for harmonizing the cybersecurity approach. To manage cyber-related risks responsibly, the

NIST Cybersecurity Framework includes guidelines, standards, and best practices. According to this framework, flexibility and affordability are of prime importance. Moreover, it aims at fostering resilience and protecting critical infrastructure by implementing the following measures:

- A better understanding, management, and reduction of the risks associated with cybersecurity.
- Prevent data loss, misuse, and restoration costs.
- Determine the most critical activities and operations that must be secured.
- Provides evidence of the trustworthiness of organizations that protect critical assets.
- Optimize the cybersecurity return on investment (ROI) by prioritizing investments.
- Responds to regulatory and contractual requirements
- Assists in the wider information security program.

Using the NIST CSF framework in conjunction with ISO/IEC 27001 simplifies the process of managing cybersecurity risk. Moreover, NIST's cybersecurity directive also allows for easier collaboration in the organization as well as across the supply chain, allowing for more effective communication.

Why cyber crime laws in India

Just like the other countries, our country is too concerned about the issue of cyber security and related crimes. Particularly in India, there are a growing number of cyber security concerns, and its responsibility to resolve them is of critical importance. It has recently been revealed that the government is losing nearly R. 1.25 lakh crore per annum to cyber-attacks overall, according to an Economic Times analysis of cyber crime.

According to another study published by Kaspersky, the number of attacks in India increased from 1.3 million to 3.3 million from the first quarter of 2020 till the end of that quarter. A total of 4.5 million attacks were recorded by India in July 2020, which was the largest number recorded so far. In July 2021, In violation of the Reserve Bank of India's directions on the storage of payment system data, Mastercard Asia/Pacific Pte Ltd (Mastercard) was banned from onboarding new domestic customers. A cyber security policy, however, does not offer an adequate method of preventing the hazards posed by the internet, and the most effective means of confronting these threats is through training. There are significant resources that the government must dedicate to safeguarding important data assets. Cyberlaw needs to be updated to incorporate the latest legal and technological developments and to address the challenges posed by the rapid development of technology.

Importance of cyber crime laws

The following points can highlight the importance of cyber laws:

- An important goal of any cyber law is to prosecute those who undertake illegal activities using the internet. To effectively prosecute these types of crimes, such as cyber abuse, assaults on other websites or individuals, theft of records, disrupting every company's online workflow, and other criminal activities, significant efforts should be undertaken, and hence, which is where cyber laws come into the picture.
- In the cases involving a violation of cyber law, the action is taken against the individual on the basis of his location and how was he involved in that violation.
- Prosecuting or retracting hackers is the most important thing since most cyber crimes are beyond the reach of a felony, which is not a crime.
- The use of the internet is also associated with security concerns and there are even some malicious individuals who want to gain unauthorised access to the computer device and commit fraud using it in the future. Hence, all rules and cyber laws are designed to protect internet businesses and internet users from unwanted unauthorized access and malicious cyber-attacks. There are a variety of ways in which individuals or associations can take action against others who commit criminal acts or break cyber laws.

Need for cyber crime laws in India

Cyberlaw is of particular importance in countries such as India, where the internet is used widely. In order to protect both individuals and organizations against cyber crime, the law was enacted. The cyberlaw allows other people or organizations to take legal action against someone if that person violates and breaks the provisions of the law.

Cyberlaw may be required in the following circumstances:

- Due to the fact that all the transactions associated with stocks are now executed in demat format, anyone who is involved with these transactions is protected by cyber law in the event of any fraudulent transactions.
- Almost all Indian companies have electronic records. A company may need this law to prevent the misuse of such data.
- As a result of the rapid development of technology, various government forms are being filled out electronically, such as income tax returns and service tax returns. Anybody can misuse those forms by hacking government portal sites, and thus, cyberlaw is required under which legal action can be taken.
- Shopping today is done through credit cards and debit cards. Unfortunately, some frauds perpetrated by means of the internet clone these credit cards and debit cards. The cloning of a credit or debit card is a technique that allows someone to obtain your information via the Internet. This can be prevented by cyberlaw as under Section 66C of the IT Act, there is 3-year imprisonment along with a fine up to one lakh rupees if anyone tries to make use of any electronic password fraudulently or dishonestly.
- Business transactions are typically carried out by means of digital signatures and electronic contracts. The misuse of digital signatures and electronic contracts can

be easily accomplished by anyone involved with them. Cyberlaw provides protection against these types of scams.

Cyber crime and security

Cybersecurity can be defined as the collection of technologies, processes, and practices that are intended to prevent networks, devices, programs, and data from being attacked, damaged or accessed by unauthorized persons. Alternatively, cyber security may also be referred to as information technology security.

Several types of organizations, including government, military, corporations, financial institutions, and medical facilities use computers and other devices to process, store, and process extremely large amounts of data. Many of those records contain sensitive data including intellectual property, financial information, personal information, etc. for which unauthorized access or exposure could have negative repercussions. There is a growing area of cyber security dedicated to protecting the systems for processing and storing sensitive information that organizations send over networks and to other devices. Thus, cybersecurity is the field dedicated to securing this sensitive information as well as the systems by which such information is transmitted or stored. With the number of cyber attacks and the sophistication of those attacks moving up, companies and organizations, especially those that are tasked with safeguarding sensitive data, (including attacks pertaining to national security, health information, or financial information), there must be steps taken for ensuring the security of their proprietary business and personnel data.

Cyber security strategies

It is also extremely important for an organisation to develop and build an effective cybersecurity strategy. The following must be included in cybersecurity strategies:

Ecosystem:

The ecosystem of an organisation needs to be strong in order to prevent cyber crime. Generally, an organisation’s ecosystem has 3 components, i.e, automation, interoperability, and authentication. By developing a safe and strong system, the organisation would be likely to protect these components and could not be attacked by malware, attrition, hacks, insider attacks, and equipment thefts.

Framework:

A framework for compliance with security standards is an assurity that can help to ensure that these standards are adhered to. Updating infrastructure is made possible as a result of this. Furthermore, it also facilitates collaboration between governments and businesses.

Open standards:

Enhanced security against cyber crime is a direct result of open standards. Through open standards, both businesses and individuals can easily implement proper security measures. These standards will also facilitate a greater level of economic growth and a broader range of new technologies.

IT mechanisms:

A variety of IT measures or mechanisms are available that can be beneficial. In the fight against cyber crime, it is essential to promote these measures and mechanisms. End-to-end protection measures, association-based protection, link-based protection, and data encryption are a few of the measures.

E-governance:

It is possible for the government to provide services online through e-governance. E-governance, however, is not taken advantage of in many countries. Cyberlaw should focus on advancing this technology to give citizens greater control.

Infrastructure:

As part of cybersecurity, protecting the infrastructure is one of the most crucial steps. This applies especially to the electrical grid as well as data transmission lines. Cyber crime is often perpetrated against outdated infrastructure.

Differences between cyber crime and cyber security

There is more to cybersecurity than just a set of guidelines and actions designed to prevent cyber crime. Ultimately, cyber-security aims to prevent hackers from finding and exploiting vulnerabilities in government and corporate networks, and therefore to make life difficult for them to do so. By contrast, cyber crime, compared to traditional crime, tends to focus more on preserving the privacy of individuals and their families while engaging in online activities.

Here is a list of the differences between cyber security and cyber crime that you should know about:

- Types of crime: The type of crime in cyber security is defined by those crimes in which a computer program, hardware, or computer network serves as the main target of an attack if it is compromised. On the other hand, cyber crime is concerned with a specific person or group of people, along with their data, as the main targets.
- Victims: Secondly, there are also differences in the types of victims in these two fields. Governments and corporations are the primary targets in cyber security while, in cyber crime, victims can range from individuals, families, organizations, governments, and corporations.

- Subject matter: Both of these fields are studied in different disciplines. Information technology, computer science, and computer engineering are the fields that cover cybersecurity. Code writing, networking and engineering are used to enhance network security. In contrast, cyber crime falls under the criminological, psychological, and sociological categories. It refers to a theory of how crime occurs and how it can be prevented.

Conclusion

With the advancement in technology, disturbing elements are appearing on the dark web that is disturbing. The Internet has become a tool of evil deeds that are exploited by intelligent people for evil motives and sometimes for financial gain. Thus, at this point in time, cyber laws come into the picture and are important for every citizen. Due to the fact that cyberspace is an extremely difficult territory to deal with, some activities are classified as grey activities that cannot be governed by law.

In India as well as across the globe, with the increasing reliance of humans on technology, cyber laws need constant up-gradation and refinement to keep pace. There has also been a significant increase in the number of remote workers as a consequence of the pandemic, which has increased the need for application security. There is a need for legislators to take extra precautions to keep ahead of the imposters so that they can act against them as soon as they arise. It can be prevented if lawmakers, internet providers, banks, shopping websites and other intercessors work together. However, ultimately, it is up to the users to participate in the fight against cyber crime. The only way for the growth of online safety and resilience to take place is through the consideration of the actions of these stakeholders, ensuring they stay within the confines of the law of cyberspace.

Organizations dealing with Cybercrime and Cyber security in India

DETAILS ABOUT INDIAN CYBERCRIME COORDINATION CENTRE (I4C) SCHEME

I Overview about the I4C Scheme

II Components of the I4C Scheme

1 National Cybercrime Threat Analytics Unit (TAU)

2 National Cybercrime Reporting Portal (www.cybercrime.gov.in)

3 Platform for Joint Cybercrime Investigation Team

4 National Cybercrime Forensic Laboratory National Cybercrime Forensic Laboratory Ecosystem

5 National Cybercrime Training Centre (NCTC) (www.cytrain.ncrb.gov.in)

6 Cybercrime Ecosystem Management Unit

7 National Cyber Crime Research and Innovation Centre

I. OVERVIEW ABOUT THE I4C SCHEME

- Outlay of Rs. 415.86 Crore

- To act as a nodal point in the fight against cybercrime
- Identify the research problems/needs of LEAs and take up R&D activities in developing new technologies and forensic tools in collaboration with academia / research institutes within India and abroad
- To prevent misuse of cyber space for furthering the cause of extremist and terrorist groups
- Suggest amendments, if required, in cyber laws to keep pace with fast changing technologies and International cooperation
- To coordinate all activities related to implementation of Mutual Legal Assistance Treaties (MLAT) with other countries related to cybercrimes in consultation with the concerned nodal authority in MHA

II. COMPONENTS OF THE I4C SCHEME

- National Cybercrime Threat Analytics Unit (TAU)
- National Cybercrime Reporting
- Platform for Joint Cybercrime Investigation Team
- National Cybercrime Forensic Laboratory (NCFL) Ecosystem
- National Cybercrime Training Centre (NCTC)
- Cybercrime Ecosystem Management Unit
- National Cyber Crime Research and Innovation Centre

1. NATIONAL CYBERCRIME THREAT ANALYTICS UNIT (TAU)

- Platform for analysing all pieces of puzzles of cybercrimes.
- Produce cybercrime threat intelligence reports and organize periodic interaction on specific cybercrime centric discussions.
- Create multi-stakeholder environment for bringing together law enforcement specialists and industry experts.

2. NATIONAL CYBERCRIME REPORTING

- Facilitate reporting of all types of cyber crime incidents with special focus on cyber crime against women and children .
- Automated routing to concerned State/UT based on information furnished in the reported incident for appropriate action in accordance with law.
- Facilitate complainants to view status of action taken on the reported incident.

3. PLATFORM FOR JOINT CYBERCRIME INVESTIGATION

- To drive intelligence-led, coordinated action against key cybercrime threats and targets.

- Facilitate the joint identification, prioritization, preparation and initiation of multi-jurisdictional action against cybercrimes.

4. NATIONAL CYBERCRIME FORENSIC LABORATORY (NCFL) ECOSYSTEM

- Forensic analysis and investigation of cybercrime as a result of new digital technology and techniques.
- A centre to support investigation process. NCFL and associated Central Forensic Science Laboratory to be well-equipped and well-staffed in order to engage in analysis and investigation activities to keep-up with new technical developments.

5. NATIONAL CYBERCRIME TRAINING CENTRE (NCTC)

- Standardization of course curriculum focused on cybercrimes, impact containment and investigations, imparting practical cybercrime detection, containment and reporting trainings on simulated cyber environments.
- Development of Massive Open Online Course on a cloud based training platform.
- National Cybercrime Training Centre to also focus on establishing Cyber Range for advanced simulation and training on cyber-attack and investigation of such cybercrimes.

6. CYBERCRIME ECOSYSTEM MANAGEMENT UNIT

- Develop ecosystems that bring together academia, industry and government to spread awareness n cyber crimes, establish standard operating procedures to contain the impact of cybercrimes and respond to cybercrimes.
- Provide support for development of all components of cybercrime combatting ecosystem.

7. NATIONAL CYBER CRIME RESEARCH AND INNOVATION CENTRE

- Track emerging technological developments, proactively predict potential vulnerabilities, which can be exploited by cybercriminals.
- To leverage the strength and expertise of all stakeholders, be it in academia, private sector or inter-governmental organizations.
- Create strategic partnerships with all such entities in the area of research and innovation focused on cybercrimes, cybercrime impact containment and investigations.

- **Steps Taken to Deal with Cyber Crime and Cyber Security**

- Central Government has taken steps to spread awareness about cyber crimes, issue of alerts/advisories, capacity building/training of law enforcement personnel/ prosecutors/ judicial officers, improving cyber forensics facilities etc. to prevent such crimes and to speed up investigation. The Government has launched the online cybercrime reporting portal, www.cybercrime.gov.in to enable complainants to report complaints pertaining to Child Pornography/Child Sexual Abuse Material, rape/gang rape imageries or sexually explicit content. The Central Government has rolled out a scheme for establishment of Indian Cyber Crime Coordination Centre (I4C) to handle issues related to cybercrime in the country in a comprehensive and coordinated manner.

- ‘Police’ and ‘Public Order’ are State subjects as per the Constitution of India. States/UTs are primarily responsible for prevention, detection, investigation and prosecution of crimes through their law enforcement machinery. The Law Enforcement Agencies take legal action as per provisions of law against the cyber crime offenders.
- Further, Government has taken several steps to prevent and mitigate cyber security incidents. These include:
- (i) Establishment of National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of critical information infrastructure in the country.
- (ii) All organizations providing digital services have been mandated to report cyber security incidents to CERT-In expeditiously.
- (iii) Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) has been launched for providing detection of malicious programmes and free tools to remove such programmes.
- (iv) Issue of alerts and advisories regarding cyber threats and counter-measures by CERT-In.
- (v) Issue of guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.
- (vi) Provision for audit of the government websites and applications prior to their hosting, and thereafter at regular intervals.
- (vii) Empanelment of security auditing organisations to support and audit implementation of Information Security Best Practices.
- (viii) Formulation of Crisis Management Plan for countering cyber attacks and cyber terrorism.
- (ix) Conducting cyber security mock drills and exercises regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors.
- (x) Conducting regular training programmes for network / system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organisations regarding securing the IT infrastructure and mitigating cyber attacks.
- This was stated by the Minister of State for Home Affairs, Shri G. Kishan Reddy in a written reply to question in the Rajya Sabha today.

Important Cyber Law Case Studies

1.Pune Citibank MphasiS Call Center Fraud

some ex employees of BPO arm of MPhasis Ltd MsourcE, defrauded US Customers of Citi Bank to the tune of RS 1.5 crores has raised concerns of many kinds including the role of "Data Protection".

The crime was obviously committed using "Unauthorized Access" to the "Electronic Account Space" of the customers. It is therefore firmly within the domain of "Cyber Crimes".

ITA-2000 is versatile enough to accommodate the aspects of crime not covered by ITA-2000 but covered by other statutes since any IPC offence committed with the use of "Electronic Documents" can be considered as a crime with the use of a "Written Documents".

"Cheating", "Conspiracy", "Breach of Trust" etc are therefore applicable in the above case in addition to section in ITA-2000.

Under ITA-2000 the offence is recognized both under Section 66 and Section 43.

Accordingly, the persons involved are liable for imprisonment and fine as well as a liability

to pay damage to the victims to the maximum extent of Rs 1 crore per victim for which the "Adjudication Process" can be invoked.

2.SONY.SAMBANDH.COM CASE

India saw its first cyber crime conviction recently. It all began after a complaint was filed by Sony India Private Ltd, which runs a website called www.sony-sambandh.com, targeting Non Resident Indians. The website enables NRIs to send Sony products to their friends and relatives in India after they pay for it online.

The company undertakes to deliver the products to the concerned recipients. In May 2002, someone logged onto the website under the identity of Barbara Campa and ordered a Sony Colour Television set and a cordless head phone. She gave her credit card number for payment and requested that the products be delivered to Arif Azim in Noida. The payment was duly cleared by the credit card agency and the transaction processed. After following the relevant procedures of due diligence and checking, the company delivered the items to Arif Azim.

At the time of delivery, the company took digital photographs showing the delivery being accepted by Arif Azim. The transaction closed at that, but after one and a half months the credit card agency informed the company that this was an unauthorized transaction as the real owner had denied having made the purchase.

The company lodged a complaint for online cheating at the Central Bureau of Investigation which registered a case under Section 418, 419 and 420 of the Indian Penal Code. The matter was investigated into and Arif Azim was arrested. Investigations revealed that Arif Azim, while working at a call centre in Noida gained access to the credit card number of an American national which he misused on the company's site.

The CBI recovered the colour television and the cordless head phone. In this matter, the CBI had evidence to prove their case and so the accused admitted his guilt. The court convicted Arif Azim under Section 418, 419 and 420 of the Indian Penal Code - this being the first time that a cybercrime has been convicted.

The court, however, felt that as the accused was a young boy of 24 years and a first-time convict, a lenient view needed to be taken. The court therefore released the accused on probation for one year. The judgment is of immense significance for the entire nation. Besides being the first conviction in a cybercrime matter, it has shown that the the Indian Penal Code can be effectively applied to certain categories of cyber crimes which are not covered under the Information Technology Act 2000. Secondly, a judgment of this sort sends out a clear message to all that the law cannot be taken for a ride.

3. The Bank NSP Case

The Bank NSP case is the one where a management trainee of the bank was engaged to be married. The couple exchanged many emails using the company computers. After some time the two broke up and the girl created fraudulent email ids such as "indianbarassociations" and sent emails to the boy's foreign clients. She used the banks computer to do this. The boy's company lost a large number of clients and took the bank to court. The bank was held liable for the emails sent using the bank's system.

4. Andhra Pradesh Tax Case

Dubious tactics of a prominent businessman from Andhra Pradesh was exposed after officials of the department got hold of computers used by the accused person. The owner of a plastics

firm was arrested and Rs 22 crore cash was recovered from his house by sleuths of the Vigilance Department. They sought an explanation from him regarding the unaccounted cash within 10 days.

The accused person submitted 6,000 vouchers to prove the legitimacy of trade and thought his offence would go undetected but after careful scrutiny of vouchers and contents of his computers it revealed that all of them were made after the raids were conducted. It later revealed that the accused was running five businesses under the guise of one company and used fake and computerised vouchers to show sales records and save tax.

5.SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra

In India's first case of cyber defamation, a Court of Delhi assumed jurisdiction over a matter where a corporate's reputation was being defamed through emails and passed an important ex-parte injunction. In this case, the defendant Jogesh Kwatra being an employ of the plaintiff company started sending derogatory, defamatory, obscene, vulgar, filthy and abusive emails to his employers as also to different subsidiaries of the said company all over the world with the aim to defame the company and its Managing Director Mr. R K Malhotra. The plaintiff filed a suit for permanent injunction restraining the defendant from doing his illegal acts of sending derogatory emails to the plaintiff.

On behalf of the plaintiffs it was contended that the emails sent by the defendant were distinctly obscene, vulgar, abusive, intimidating, humiliating and defamatory in nature. Counsel further argued that the aim of sending the said emails was to malign the high reputation of the plaintiffs all over India and the world. He further contended that the acts of the defendant in sending the emails had resulted in invasion of legal rights of the plaintiffs. Further the defendant is under a duty not to send the aforesaid emails. It is pertinent to note that after the plaintiff company discovered the said employ could be indulging in the matter of sending abusive emails, the plaintiff terminated the services of the defendant.

After hearing detailed arguments of Counsel for Plaintiff, Hon'ble Judge of the Delhi High Court passed an ex-parte ad interim injunction observing that a prima facie case had been made out by the plaintiff. Consequently, the Delhi High Court restrained the defendant from sending derogatory, defamatory, obscene, vulgar, humiliating and abusive emails either to the plaintiffs or to its sister subsidiaries all over the world including their Managing Directors and their Sales and Marketing departments. Further, Hon'ble Judge also restrained the defendant from publishing, transmitting or causing to be published any information in the actual world as also in cyberspace which is derogatory or defamatory or abusive of the plaintiffs.

This order of Delhi High Court assumes tremendous significance as this is for the first time that an Indian Court assumes jurisdiction in a matter concerning cyber defamation and grants an ex-parte injunction restraining the defendant from defaming the plaintiffs by sending derogatory, defamatory, abusive and obscene emails either to the plaintiffs or their subsidiaries.

6. Bazee.com case

CEO of Bazee.com was arrested in December 2004 because a CD with objectionable material was being sold on the website. The CD was also being sold in the markets in Delhi.

The Mumbai city police and the Delhi Police got into action. The CEO was later released on bail. This opened up the question as to what kind of distinction do we draw between Internet

Service Provider and Content Provider. The burden rests on the accused that he was the Service Provider and not the Content Provider. It also raises a lot of issues regarding how the police should handle the cyber crime cases and a lot of education is required.

7. State of Tamil Nadu Vs Suhas Katti

The Case of Suhas Katti is notable for the fact that the conviction was achieved successfully within a relatively quick time of 7 months from the filing of the FIR. Considering that similar cases have been pending in other states for a much longer time, the efficient handling of the case which happened to be the first case of the Chennai Cyber Crime Cell going to trial deserves a special mention.

The case related to posting of obscene, defamatory and annoying message about a divorcee woman in the yahoo message group. E-Mails were also forwarded to the victim for information by the accused through a false e-mail account opened by him in the name of the victim. The posting of the message resulted in annoying phone calls to the lady in the belief that she was soliciting.

Based on a complaint made by the victim in February 2004, the Police traced the accused to Mumbai and arrested him within the next few days. The accused was a known family friend of the victim and was reportedly interested in marrying her. She however married another person. This marriage later ended in divorce and the accused started contacting her once again. On her reluctance to marry him, the accused took up the harassment through the Internet.

On 24-3-2004 Charge Sheet was filed u/s 67 of IT Act 2000, 469 and 509 IPC before The Hon'ble Addl. CMM Egmore by citing 18 witnesses and 34 documents and material objects. The same was taken on file in C.C.NO.4680/2004. On the prosecution side 12 witnesses were examined and entire documents were marked as Exhibits.

The Defence argued that the offending mails would have been given either by ex-husband of the complainant or the complainant her self to implicate the accused as accused alleged to have turned down the request of the complainant to marry her.

Further the Defence counsel argued that some of the documentary evidence was not sustainable under Section 65 B of the Indian Evidence Act. However, the court relied upon the expert witnesses and other evidence produced before it, including the witnesses of the Cyber Cafe owners and came to the conclusion that the crime was conclusively proved.

Ld. Additional Chief Metropolitan Magistrate, Egmore, delivered the judgement on 5-11-04 as follows:"The accused is found guilty of offences under section 469, 509 IPC and 67 of IT Act 2000 and the accused is convicted and is sentenced for the offence to undergo RI for 2 years under 469 IPC and to pay fine of Rs.500/-and for the offence u/s 509 IPC sentenced to undergo 1 year Simple imprisonment and to pay fine of Rs.500/- and for the offence u/s 67 of IT Act 2000 to undergo RI for 2 years and to pay fine of Rs.4000/- All sentences to run concurrently.

"The accused paid fine amount and he was lodged at Central Prison, Chennai. This is considered as the first case convicted under section 67 of Information Technology Act 2000 in India.

8. Nasscom vs. Ajay Sood & Others

In a landmark judgment in the case of National Association of Software and Service Companies vs Ajay Sood & Others, delivered in March, '05, the Delhi High Court declared

'phishing' on the internet to be an illegal act, entailing an injunction and recovery of damages. Elaborating on the concept of 'phishing', in order to lay down a precedent in India, the court stated that it is a form of internet fraud where a person pretends to be a legitimate association, such as a bank or an insurance company in order to extract personal data from a customer such as access codes, passwords, etc. Personal data so collected by misrepresenting the identity of the legitimate party is commonly used for the collecting party's advantage. court also stated, by way of an example, that typical phishing scams involve persons who pretend to represent online banks and siphon cash from e-banking accounts after conning consumers into handing over confidential banking details.

The Delhi HC stated that even though there is no specific legislation in India to penalize phishing, it held phishing to be an illegal act by defining it under Indian law as "a misrepresentation made in the course of trade leading to confusion as to the source and origin of the e-mail causing immense harm not only to the consumer but even to the person whose name, identity or password is misused." The court held the act of phishing as passing off and tarnishing the plaintiff's image.

The plaintiff in this case was the National Association of Software and Service Companies (Nasscom), India's premier software association.The defendants were operating a placement agency involved in head-hunting and recruitment. In order to obtain personal data, which they could use for purposes of headhunting, the defendants composed and sent e-mails to third parties in the name of Nasscom.

The high court recognised the trademark rights of the plaintiff and passed an ex-parte adinterim injunction restraining the defendants from using the trade name or any other name deceptively similar to Nasscom. The court further restrained the defendants from holding themselves out as being associates or a part of Nasscom.

The court appointed a commission to conduct a search at the defendants' premises. Two hard disks of the computers from which the fraudulent e-mails were sent by the defendants to various parties were taken into custody by the local commissioner appointed by the court. The offending e-mails were then downloaded from the hard disks and presented as evidence in court.

During the progress of the case, it became clear that the defendants in whose names the offending e-mails were sent were fictitious identities created by an employee on defendants' instructions, to avoid recognition and legal action. On discovery of this fraudulent act, the fictitious names were deleted from the array of parties as defendants in the case.

Subsequently, the defendants admitted their illegal acts and the parties settled the matter through the recording of a compromise in the suit proceedings. According to the terms of compromise, the defendants agreed to pay a sum of Rs1.6 million to the plaintiff as damages for violation of the plaintiff's trademark rights. The court also ordered the hard disks seized from the defendants' premises to be handed over to the plaintiff who would be the owner of the hard disks.

This case achieves clear milestones: It brings the act of "phishing" into the ambit of Indian laws even in the absence of specific legislation; It clears the misconception that there is no "damages culture" in India for violation of IP rights; This case reaffirms IP owners' faith in the Indian judicial system's ability and willingness to protect intangible property rights and

send a strong message to IP owners that they can do business in India without sacrificing their IP rights.

Unit 3

Social Media overview and Security

What is social networking?

Social networks are websites and apps that allow users and organizations to connect, communicate, share information and form relationships. People can connect with others in the same area, families, friends, and those with the same interests. Social networks are one of the most important uses of the internet today.

Popular social networking sites -- such as Facebook, Yelp, Twitter, Instagram and TikTok -- enable individuals to maintain social connections, stay informed and access, as well as share a wealth of information. These sites also enable marketers to reach their target audiences.

Social networking sites have come a long way since the first social networking site, SixDegrees.com, was launched in 1997. Today, the world is rapidly adopting newer social networking platforms. According to DataReportal, a Kepios analysis from January 2022 indicated that there are more than 4.74 billion social network users worldwide.

How does social networking work?

The term *social networking* entails having connections in both the real and the digital worlds. Today, this term is mainly used to reference online social communications. The internet has made it possible for people to find and connect with others who they may never have met otherwise.

Online social networking is dependent on technology and internet connectivity. Users can access social networking sites using their PCs, tablets or smartphones. Most social networking sites run on a back end of searchable databases that use advanced programming languages, such as Python, to organize, store and retrieve data in an easy-to-understand format. For example, Tumblr uses such products and services in its daily operations as Google Analytics, Google Workspace and WordPress.

What are social networks?

With the broad spectrum of websites, apps and services that exist online, there is no single exact definition of a social network. Generally, though, social networks have a few common attributes that set them apart.

- A social network will focus on user-generated content. Users primarily view and interact with content made by other users. They are encouraged to post text, status updates or pictures for viewing by others.
- Social networks allow the user or organization to create a profile. The profile contains information about the person and a centralized page with the content posted by them. Their profile may be associated with their real name.
- A social network has a way to form a lasting connection with other users. These connections are commonly called *friending* or *following* the other user. They allow the users to find other users and form webs of relationships. Often an algorithm will recommend other users and organizations they may want to form a connection with.

Although often used interchangeably, social network is different than social media. A social network focuses on the connections and relationships between individuals. Social media is more focused on an individual sharing with a large audience. In this case, *media* is used in the same sense as in mass media. Most social networks can also be used as social media sites.

What is the purpose of social networking?

Social networking fulfills the following four main objectives:

- **Sharing.** Friends or family members who are geographically dispersed can connect remotely and share information, updates, photos and videos. Social networking also enables individuals to meet other people with similar interests or to expand their current social networks.
- **Learning.** Social networks serve as great learning platforms. Consumers can instantly receive breaking news, get updates regarding friends and family, or learn about what's happening in their community.

- **Interacting.** Social networking enhances user interactions by breaking the barriers of time and distance. With cloud-based video communication technologies such as WhatsApp or Instagram Live, people can talk face to face with anyone in the world.
- **Marketing.** Companies may tap into social networking services to enhance brand awareness with the platform's users, improve customer retention and conversion rates, and promote brand and voice identity.

What are the different types of social networking?

While there are various categories of social networking sites, the six most common types are the following:

- **Social connections.** This is a type of social network where people stay in touch with friends, family members, acquaintances or brands through online profiles and updates, or find new friends through similar interests. Some examples are Facebook, Myspace and Instagram.
- **Professional connections**. Geared toward professionals, these social networks are designed for business relationships. These sites can be used to make new professional contacts, enhance existing business connections and explore job opportunities, for example. They may include a general forum where professionals can connect with co-workers or offer an exclusive platform based on specific occupations or interest levels. Some examples are LinkedIn, Microsoft Yammer and Microsoft Viva.
- **Sharing of multimedia.** Various social networks provide video- and photography-sharing services, including YouTube and Flickr.
- **News or informational.** This type of social networking allow users to post news stories, informational or how-to content and can be general purpose or dedicated to a single topic. These social networks include communities of people who are looking for answers to everyday problems and they have much in common with web forums. Fostering a sense of helping others, members provide answers to questions, conduct discussion forums or teach others how to perform various tasks and projects. Popular examples include Reddit, Stack Overflow or Digg.
- **Communication.** Here, social networks focus on allowing the user to communicate directly with each other in one-on-one or group chats. They have less focus on posts

or updates and are like instant messaging apps. Some examples are WhatsApp, WeChat and Snapchat.

- **Educational.** Educational social networks offer remote learning, enabling students and teachers to collaborate on school projects, conduct research, and interact through blogs and forums. Google Classroom, LinkedIn Learning and ePals are popular examples.

What are the advantages and disadvantages of social networking?

Social networking can be a double-edged sword. On one end, it provides unsurpassed social benefits, yet it can also make people more vulnerable to the spread of misinformation, as well as privacy and security threats.

Social networking offers the following benefits to consumers and businesses:

- **Brand awareness.** Social networking enables companies to reach out to new and existing clients. This helps to make brands more relatable and promotes brand awareness.
- **Instant reachability.** By erasing the physical and spatial boundaries between people, social networking websites can provide instant reachability.
- **Builds a following.** Organizations and businesses can use social networking to build a following and expand their reach globally.
- **Business success.** Positive reviews and comments generated by customers on social networking platforms can help improve business sales and profitability.
- **Increased website traffic.** Businesses can use social networking profiles to boost and direct inbound traffic to their websites. They can achieve this, for example, by adding inspiring visuals, using plugins and shareable social media buttons, or encouraging inbound linking.

Social networking also has the following downsides:

- **Rumors and misinformation.** Incorrect information can slip through the cracks of social networking platforms, causing havoc and uncertainty among consumers.

Often, people take anything posted on social networking sites at face value instead of verifying the sources.

- **Negative reviews and comments.** A single negative review can adversely affect an established business, especially if the comments are posted on a platform with a large following. A tarnished business reputation can often cause irreparable damage.
- **Data security and privacy concerns.** Social networking sites can inadvertently put consumer data at risk. For instance, if a social networking site experiences a data breach, the users of that platform automatically fall under the radar as well. According to Business Insider, a data breach in April 2021 leaked the personal data of more than 500 million Facebook users.
- **Time-consuming process.** Promoting a business on social media requires constant upkeep and maintenance. Creating, updating, preparing and scheduling regular posts can take a considerable amount of time. This can be especially cumbersome for small businesses that may not have the extra staff and resources to dedicate to social media marketing.

Social networks in business

There are many ways a business or organization can use social networks. Globally, the average person spends over two hours a day using social networks. This represents a great opportunity and market.

Most social networks are run as for-profit companies. They make most of their revenue from selling ads or promoted content. Facebook's parent company Meta has an almost $300 billion market cap.

Social networks can be used for customer research, engagement and marketing. They offer a way to directly connect businesses and customers. Brands can build a community around themselves. Social networks collect information about users' likes and dislikes, allowing for extremely targeted advertising. Social media listening allows an organization to learn what people are saying about their company.

Some businesses are implementing internal social networks. In very large organizations this can increase employee engagement and satisfaction. Also, as teams become more

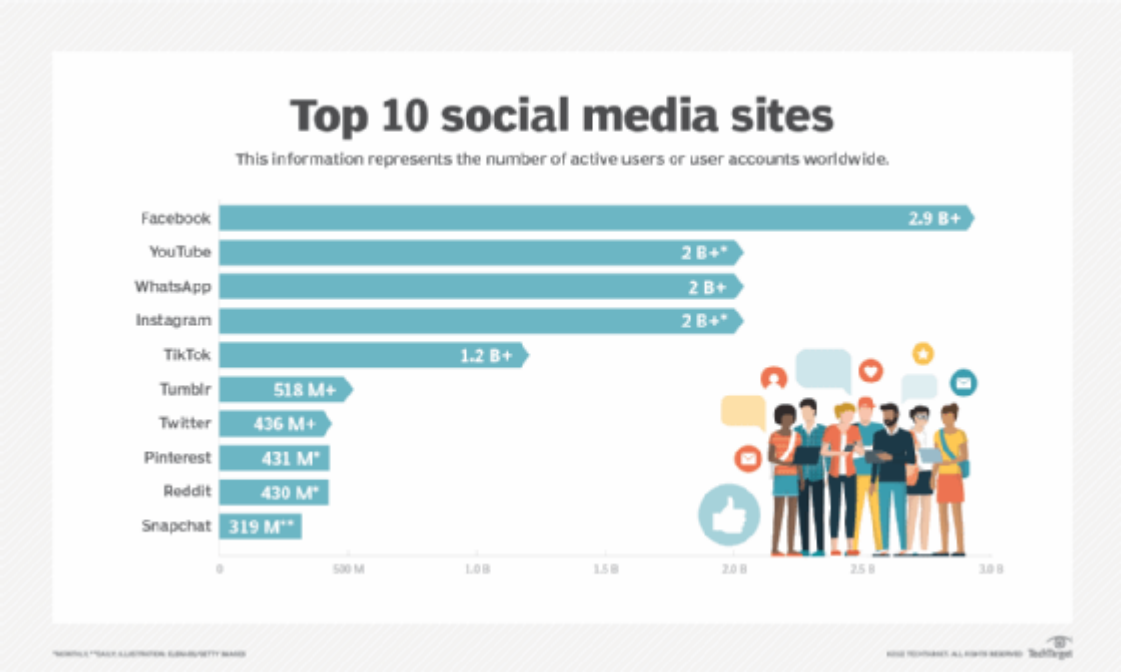
geographically diverse or have members working from home, private social networks can promote collaboration and information sharing.

Some business are beginning to use social networks in their recruitment strategies.

Examples of social networking

Every established organization advertises on social networking these days. Here are four examples of social networking websites:

- **Yelp.** Picking a restaurant, dentist, doctor or hair salon is not always easy, so social networking sites like Yelp offer crowdsourced customer reviews of these types of businesses or providers.
- **Pinterest.** Bookmarking sites like Pinterest enable users to share photos and organize links to a variety of online resources and websites. Similar to a digital scrapbook, Pinterest enables users to save specific *pins* to *pinboards*, making it easier to search for specific topics and share them with followers.
- **Rover.** A popular pet-sitter services portal, Rover enables pet owners to connect with pet sitters, dog walkers and pet-boarding services.
- **Airbnb.** Airbnb helps travelers search for a place to stay based on their preferences, including multishared spaces, shared spaces with private rooms and entire properties. Places on Airbnb are mostly rented out by homeowners.



These 10 popular social networking websites share millions to billions of users.

What are the top 10 social networking sites or platforms?

Although there are numerous social networking websites, the following sites are the most popular:

1. **Facebook.** Facebook users create profiles, share information, send messages and post status updates on their *walls*. Ranked the most active social networking platform by DataReportal, Facebook has more than 2.9 billion active users. In 2021, the company was renamed Meta to reflect its business beyond just social media.
2. **YouTube.** This popular video-sharing website enables users to share, upload and post videos and vlogs. According to Global Media Insight, YouTube has more than 2 billion monthly active users.
3. **WhatsApp.** This free instant messaging app lets users send text messages, make video and voice calls, and share documents. According to WhatsApp, it has more than 2 billion users worldwide.
4. **Instagram.** This free social media platform enables users to share long- and short-form videos and photos. It is primarily designed for iOS and Android smartphone users, but a desktop version is also available. However, sharing and uploading of content is only available through the Instagram app. Also owned by Meta, Instagram has over 2 billion monthly active users as of December 2021, according to CNBC.

5. **TikTok.** This app is used for sharing and making personalized short videos. TikTok caters to a younger audience and is well known for being a lively and fun-to-use social networking platform. According to the *Business of Apps* newsletter, TikTok has more than 1.2 billion users as of the end of 2021.

6. **Tumblr.** This microblogging site enables users to publish multimedia and other content types inside short blog posts. Users can also follow other users and make their blogs private. According to FinancesOnline, as of February 2021, Tumblr has more than 518 million user accounts.

7. **Twitter.** Launched in 2006, this social media platform enables users to share their thoughts and opinions with a broad audience by posting messages known as *tweets* that contain up to 280 characters. According to DataReportal, as of January 2022, Twitter has more than 436 million users.

8. **Pinterest.** The Pinterest bookmarking site enables users to save and organize links to favorite online resources and destinations through *tagging*. According to Pinterest Inc., the platform has 431 million global monthly active users as of December 2021 -- a 6% decrease over the previous year.

9. **Reddit.** Founded in 2005, Reddit provides a diverse collection of forums and subforums -- also known as subreddits -- on a variety of topics, including sports, breaking news and technology. Here, users can comment on each other's posts, as well as share news and content. According to Reddit, it has more than 50 million daily active users. This translates into 430 million monthly users as of 2019, according to *The Small Business Blog*.

10. **Snapchat.** This multimedia app can be used on smartphones running Android or iOS. Founded in 2011, Snapchat enables users to send pictures or videos called *snaps* to friends. These snaps vanish after they have been viewed. According to Snap Inc., Snapchat has 319 million daily active users as of the end of 2021.

Social Media Monitoring

Social media monitoring is the process of identifying and analysing mentions of a certain brand or product through different social media platforms, forums and other websites.

Why is social media monitoring important?

When brands use social media monitoring, they can do the following things.

- **Analyze direct mentions of a brand**. You can collect direct @mentions across social media to easily react to customer behavior and deliver value at the right time.
- **Analyze indirect mentions**. You can see public messages and comments from all around the web that only include a variation of your brand's name, with no hashtags whatsoever. This allows you to understand the context.
- **Spend less time on manual data collection**. If you analyze brand mentions across all social media where your business is present, you will probably have to switch between many apps and manually search for mentions to stay on top of it. Social media monitoring tools (which we will discuss later in the article) allow companies to automate this time-consuming process.
- **Improve customer care strategies**. It can lead to faster response times, prevent public relations issues and identify brand advocates. Improving your customer care strategy increases customer loyalty and brand awareness.
- **Improve overall marketing strategy**. Insights gained from social media monitoring help brands improve relationships with potential customers and quickly respond to their behavior, reactions, needs, pain points, and desires. This data can be used later for strengthening your communication, improving content quality and selling strategies.

Let's find out the benefits of using social media monitoring.

Benefits of Social Media Monitoring

Social media monitoring helps companies get the idea of their company's public perception, which allows them to:

- react to consumers' behavior on social platforms in real time;
- determine how certain demographics feel about your brand;
- use positive feedback as a social proof in your strategy;
- use negative feedback to solve issues at any buyer's journey stage;
- build brand credibility and authenticity;
- eliminate channels with the lowest engagement levels to save money and effort;
- analyze performance of different social media marketing campaigns;

- calculate return on investment through advanced reporting capabilities.

Let's discover the principles according to which social media monitoring works.

How does social media monitoring work?

Social media monitoring works similar to search engines like Google and Bing. The robot crawls social media platforms in search of predefined keywords. This activity is completely legal and compliant with GDPR laws.

No matter what tool you choose, there are three key processes in social media monitoring:

1. **Setting-up**. First of all, you need to set up a project where you list the keywords you want to track across the internet and social media. It can be your brand's name, product names and combinations of both. An advanced setup may require excluded keywords to make an even more specific inquiry.
2. **Collecting**. The tool collects mentions into a dashboard report. It usually offers plenty of filters to clean up, group, mark and delete collected mentions. Social media monitoring tool also allows you to receive mentions directly to your inbox in a format of real-time, daily, and weekly reports.
3. **Analyzing**. Data analysis varies between different tools. Some tools focus on volume, engagement and reach metrics, the others — on sentiment and influence of social media mentions.

These three processes are the core of social media monitoring. Once you have your keywords in place, the service collects mentions and comments across the internet and provides metrics that will help you better understand the context and come up with correct reactions at the right time.

A process that follows is creating a strategy based on social media monitoring insights, which is called "listening." Let's find out the difference between social media monitoring and listening.

Social Media Monitoring vs. Listening

These processes are equally important parts of collecting feedback from the audience. The main difference between them is that social media monitoring is just a process of collecting and sorting mentions while listening is the actual analysis of those insights with intention to build a better marketing strategy based on this data.

Besides, monitoring can be automated, while social media listening requires a lot of manual work and thoughtful analysis, creativity, and ability to deeply understand user intentions and emotions behind their behavior on social media.

Social media listening is an important research tool that is meant for analyzing user interactions with your brand across the internet and finding the ways to put what you learn into action. That can be something as small as responding to a happy customer, or something as big as shifting your entire brand positioning. Marketers often use this tool to analyze their competitors, discover new sales leads, and identify influencers and brand advocates.

Just like social media monitoring, there are services that provide tools for listening. These services usually provide tools for both processes, that's why it's best to regard them as an integrated whole, because none of them makes sense without another.

Let's review some tools that will help you succeed at social media monitoring.

Social Media Monitoring Tools

We've collected three popular social media monitoring services.

Hootsuite

Monitoring tool is one of many social media management tools available at Hootsuite. With Hootsuite, you can set up automated crawls of social media content based on your mentions, selected keywords, hashtags, and locations. It also provides real-time audience insights to help you identify what the audience feels about your brand, detect thought leaders, and get immediate alerts if there are suspicious numbers of mentions. Furthermore, Hootsuite integrates with more than a hundred apps to add more functions to its dashboard.

Below there is a Hootsuite dashboard which includes brand mentions on Twitter.

Platforms supported: Instagram, Facebook, Twitter, YouTube, LinkedIn, Pinterest, blogs, forums, etc.

Pricing: The Professional plan offers a 30-day free trial and $19 per month after expiration. It allows you to connect one user and up to 10 social media accounts. Unlimited post scheduling and aggregated inbox for messaging are the features available on any plan.

The Team plan costs $99 per month with up to three users and 20 social media accounts, as well as management tools for the team, such as assignment of specific comments to different team members.

The Business plan costs $599 per month with over 5 users, 35 social media accounts, 24/7 priority support, integrations with Zendesk, Slack, Basecamp, etc.

The Enterprise plan offers custom solutions and more additional features such as quarterly business reviews and reports on the team's performance.You can find more details on Hootsuite pricing page.

Sprout Social

Similar to Hootsuite, Sprout Social's monitoring and engagement tools are part of its social media management software. Sprout Social provides two separate features for social monitoring and engagement.

In the Smart Inbox, you'll get all your social media mentions and messages. The discovery feature allows you to search for particular keywords on Twitter or Instagram, including mentions without tagging your social media profile.

Below there is a social media monitoring report in the form of a calendar. You can see comments and mentions across social media platforms as well as the number of daily interactions with a brand.

Platforms supported: Twitter, Facebook, Instagram, LinkedIn, and YouTube.

Prices: All plans have a 30-day free trial. *The Standard plan* costs $99 per month with 5 social media profiles to connect, all-in-one social inbox, crafting and publishing posts, profiles, keywords, and location monitoring and more.

The Professional plan costs $149 per month with 10 social media profiles to connect, includes all features from the Standard plan plus competitive reports for Instagram, Facebook, and Twitter, incoming and outcoming message content tagging, custom workflows for multiple approvers and steps, and more.

The Advanced plan costs $249 per month with 10 social media profiles to connect, all features from the Professional plan, Message Spike Alerts for increased message activity, digital asset and content library, chatbots with automation tools, saved and suggested replies, Automated Link Tracking and more. You can find more information on Sprout Social pricing page.

Agora Pulse

Agora Pulse is an all-in-one social media management tool, which has scheduling, monitoring, engagement, and analytics features. All your social media mentions are collected in the inbox, while its listening feature allows you to search for keywords, URL, and handle on Twitter. Agora Pulse also allows you to monitor comments on your Facebook and Instagram ads.

Below you can see the dashboard, where you can quickly respond to customer comments across various social media platforms.

Platforms supported: Facebook, Twitter, Instagram, LinkedIn, YouTube.

Pricing: The service offers a 30-day free trial. *The Pro plan* costs $79 per month with 2 users and up to 10 social media accounts to connect.

The Premium plan costs $159 per month with 4 users and up to 25 social media profiles to connect.

The Enterprise plan has custom pricing options with 8+ users and 40+ social media accounts to connect. You can find more information on Agora Pulse pricing page.

Let’s find out how to begin monitoring user activities across your social media channels.

How to get started with social media monitoring?

Here are steps to begin and succeed at social media monitoring.

1. **Choose a social media monitoring platform**. Consider pricing and functionality that is crucial for your business. Make sure that a social media monitoring service of your choice specializes on platforms where your business works. You can use free trials and request demos to better understand how certain services work to make the right choice.
2. **List the relevant keywords for crawling**. Make up a list of keywords based on your brand name, including possible misspellings. You can also include product names that are connected with your brand and add keywords related to your competitors in case you want to analyze their responses to customers across social media platforms.

3. **Prioritize the processes.** Since social media monitoring includes many different processes you should correctly prioritize them. The most important thing is to solve negative issues as soon as they appear. It's especially harmful when it goes viral, so it's best to take control over such situations right away. The next key aspect of monitoring social media is to communicate with people who mention your brand in a positive context. This will help you collect more leads, establish a good reputation, and build rapport with your audience.
4. **Use the service's functionality to the maximum extent**. Try to utilize available features to get the most out of social media monitoring. Once you feel that results are not satisfying or available functionality does not meet your needs, consider changing a plan or switch to another service, which offers the right tools for you.
5. **Create an effective strategy.** You need to find ways to deal with all mentions across social media and provide as much value to the audience as possible. A great strategy must be a combination of social media marketing, monitoring, and listening. It all starts when you create relevant and engaging content. Then people react to it and you collect and analyze those reactions. Lastly, you need to respond to both positive and negative feedback because it will improve your chances to make a good public impression and create more buzz around your brand and products.

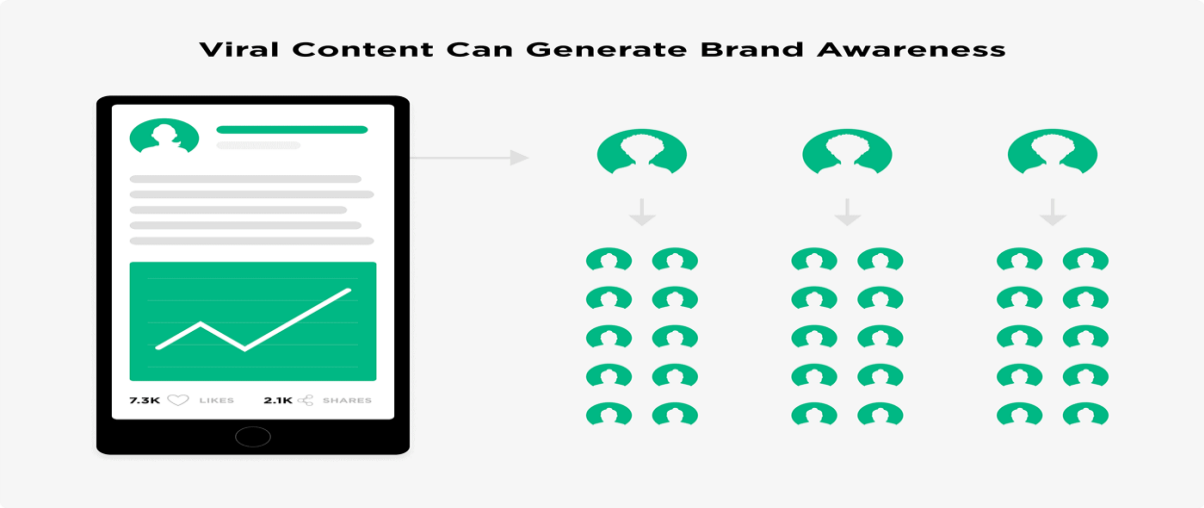
Viral Content

What Is Viral Content?

Viral content is online content that achieves a high level of awareness due to shares and exposure on social media networks, news websites, aggregators, email newsletters and search engines.

Why Is Viral Content Important?

A single piece of viral content can generate significant amounts of brand awareness and traffic to your website.

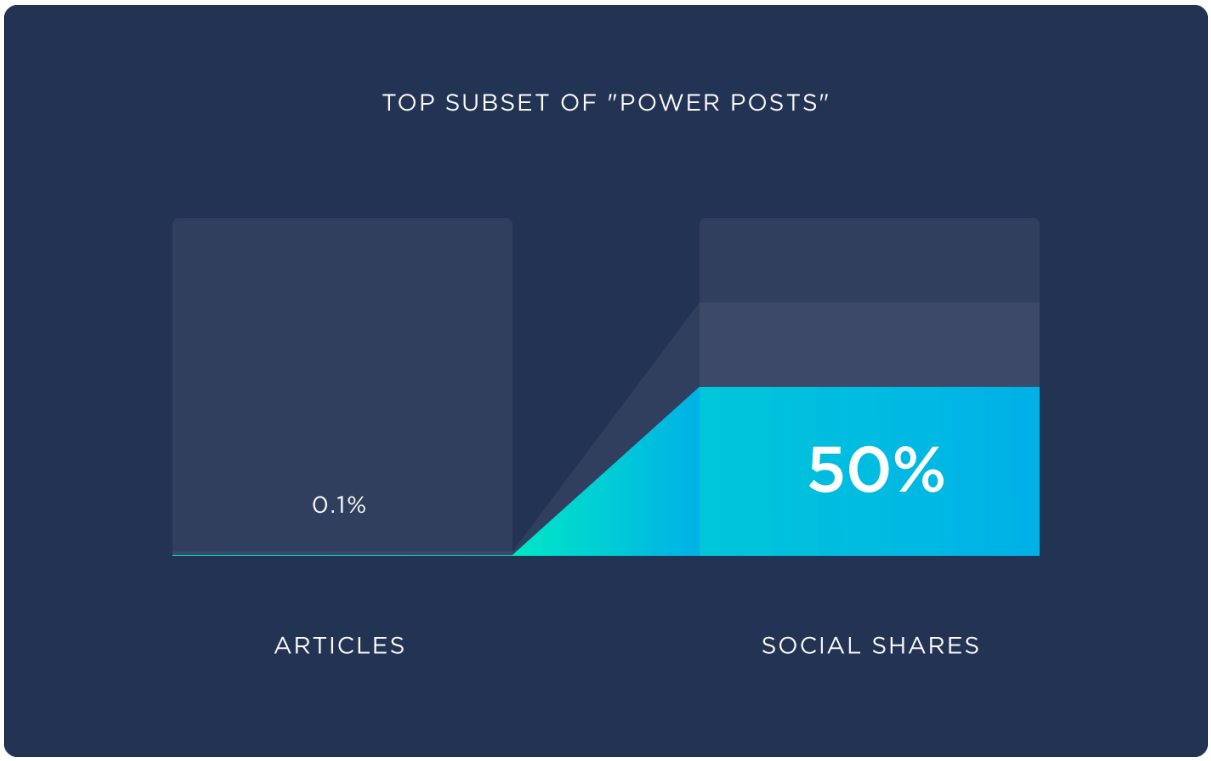


And because most of the traffic that you get comes from social shares, viral content is relatively cheap compared to paid ads.

But there's a catch:

Viral content is tough to pull off.

In fact, a content marketing study that we ran discovered that a small percentage of content (called "Power Posts") drive most social sharing.



In other words: most content gets virtually zero shares. But a few top performers tend to dominate.

So how do you get your content to go viral? Check out these best practices.

Best Practices

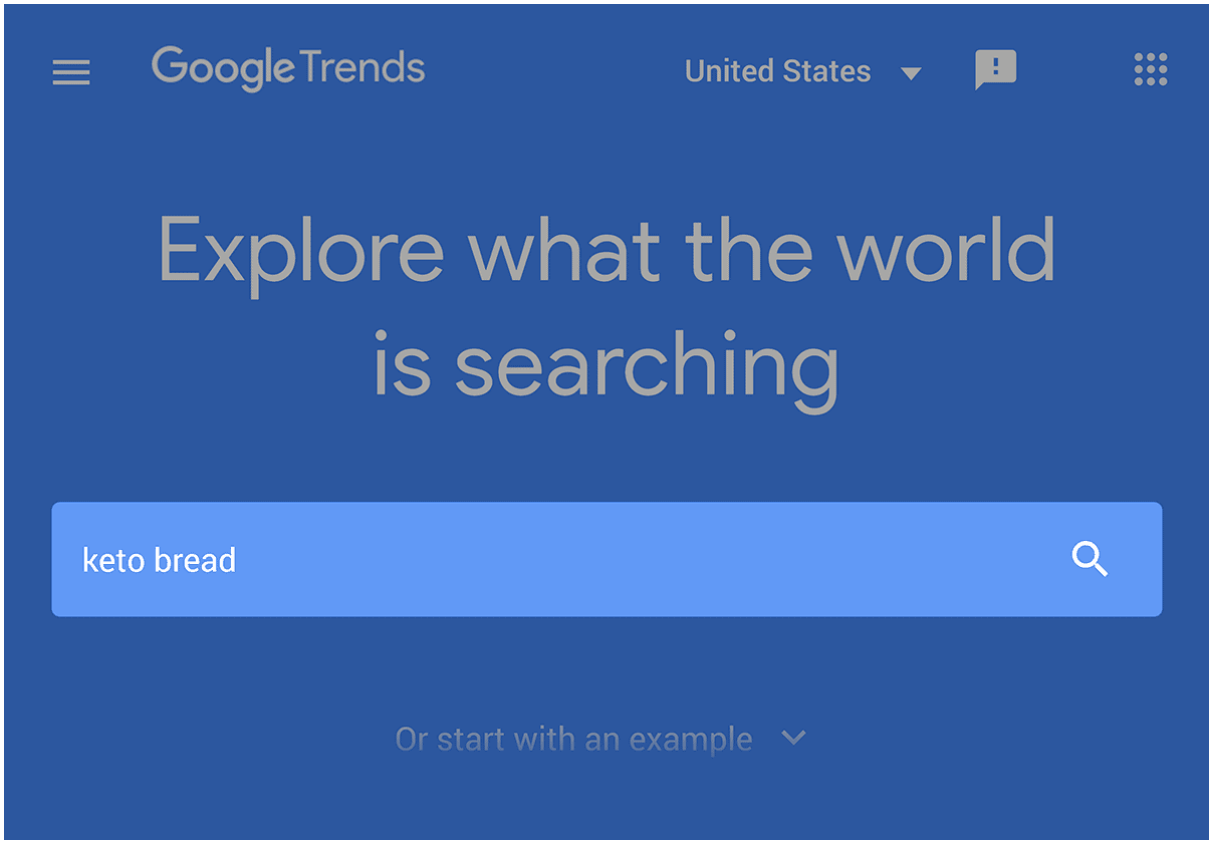
Focus On Trending Topics

When it comes to viral content, your topic is KEY.

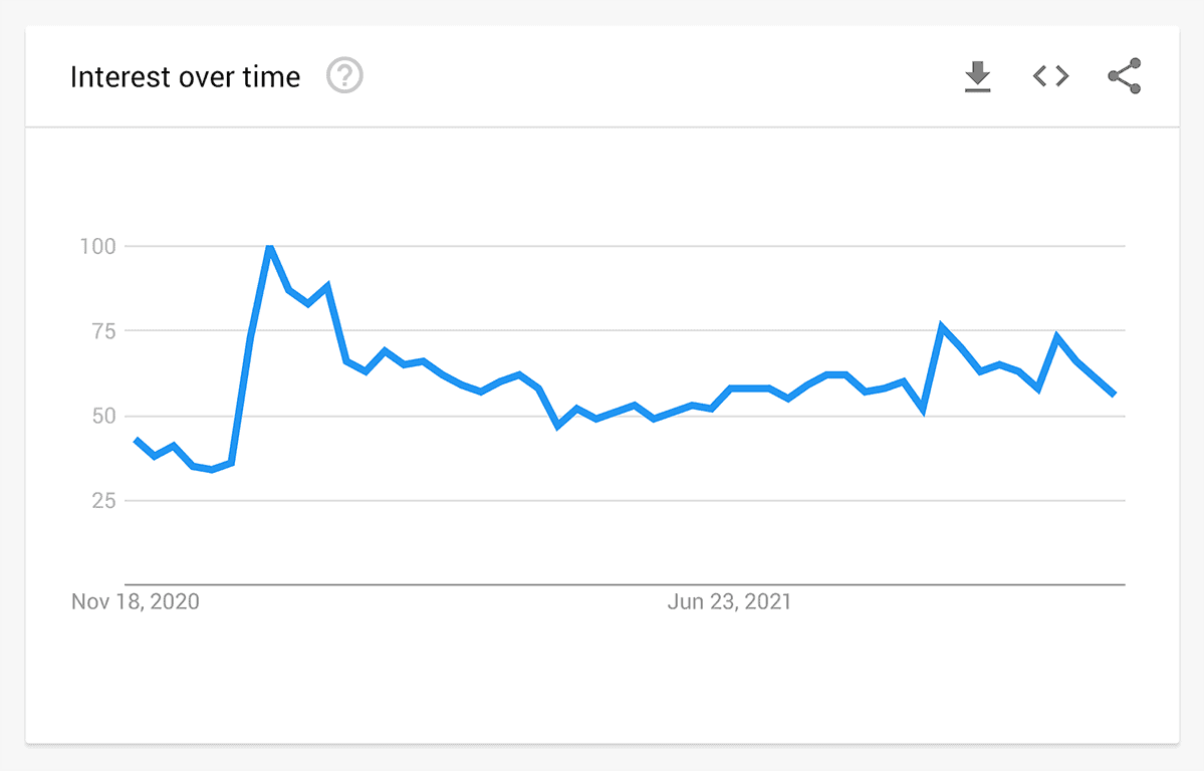
Specifically, you want to create your content around a topic that's blowing up. That way, you can ride the wave.

And the best way to find growing topics? Google Trends.

All you need to do is type in the topic you want to write about.



If interest in that topic is growing, that's a good sign.



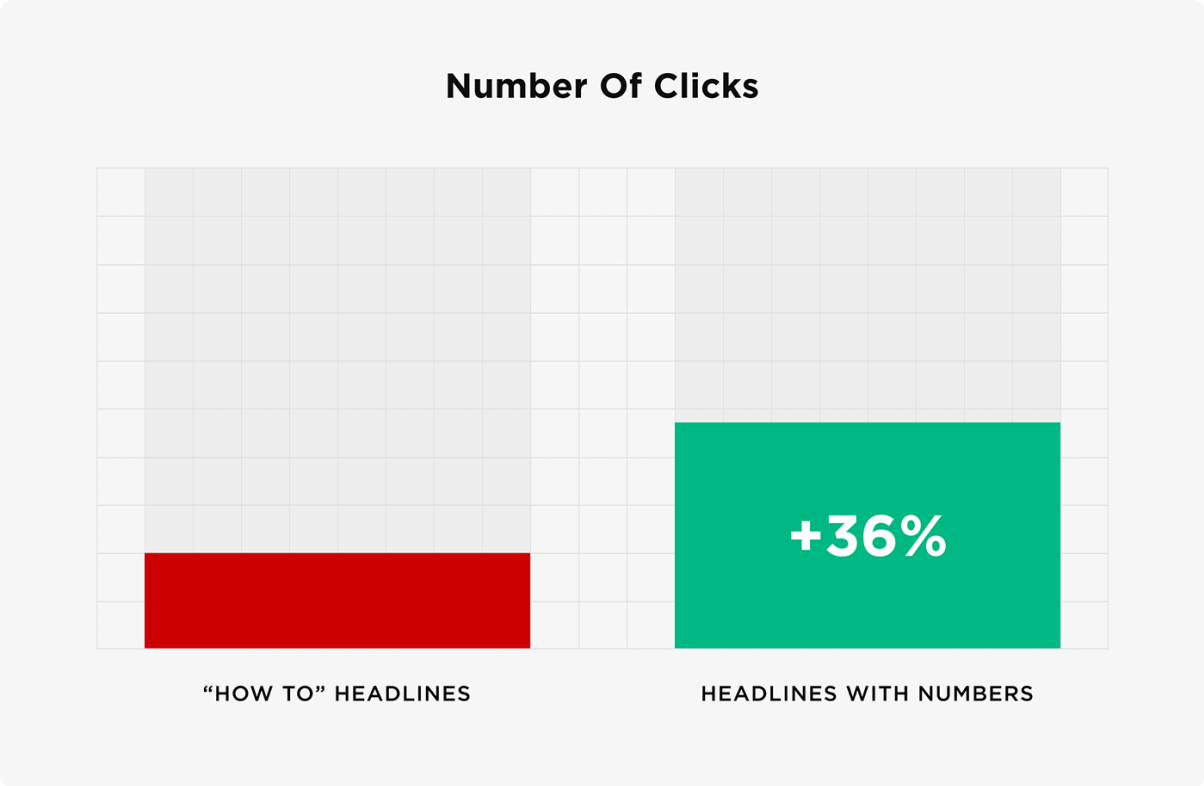
If not, you probably want to go with a different topic.

Write Viral Headlines

When someone sees your content getting shared on Twitter, Facebook and other social sites, your title is what ultimately pushes them to click.

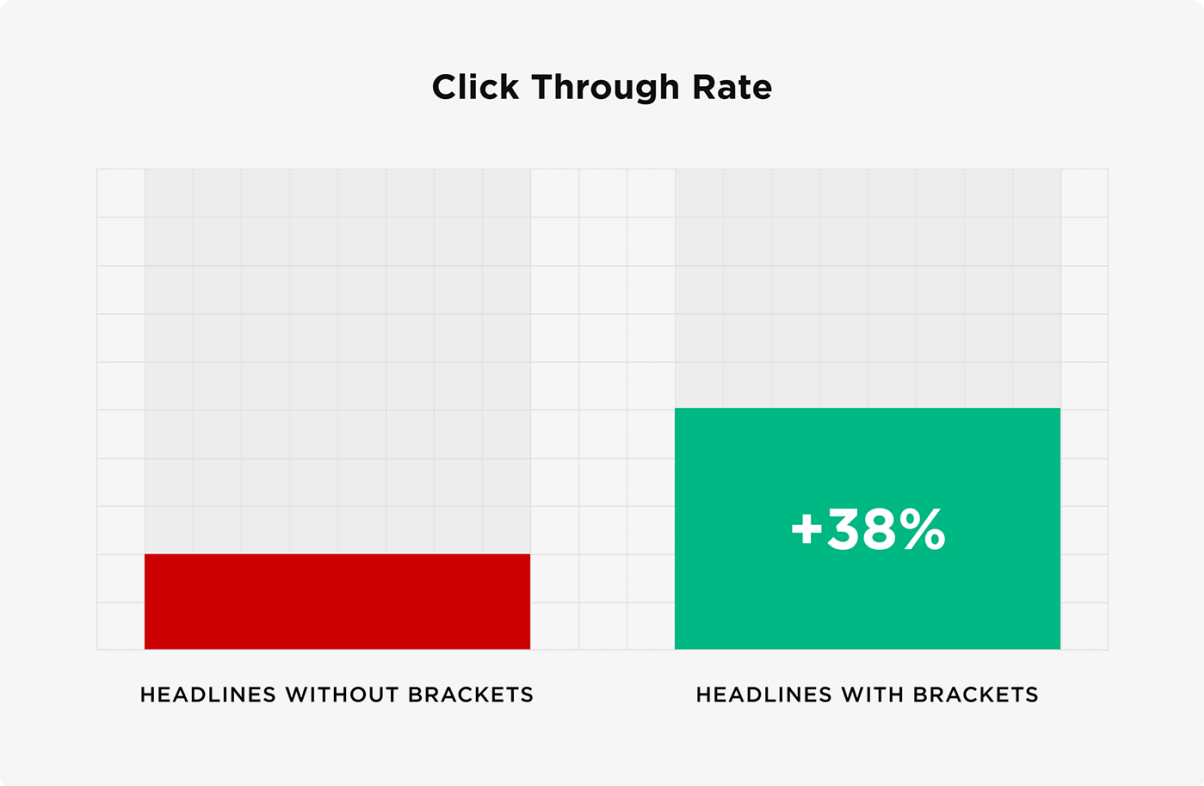
So while your content itself is super important, your title can make or break how your post does.

According to research by Conductor, headlines with numbers are 36% more likely to generate clicks.



So whenever it makes sense, use a specific number in your title.

HubSpot reports that adding brackets to your headlines can also lead to more clicks and shares.

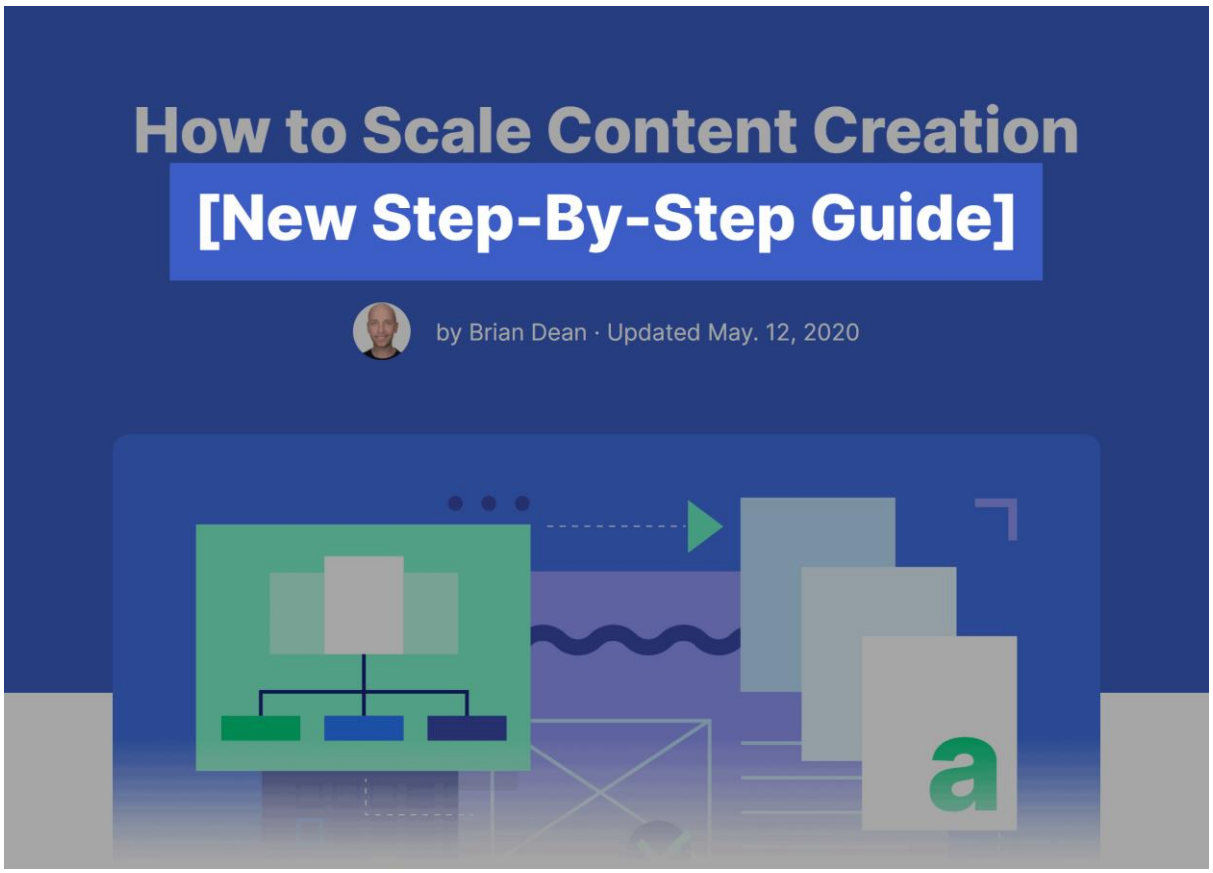


Brackets give people a “sneak preview” of your post.

Is your post an infographic? A case study? A video?

Brackets let people know… before they click.

For example, here's the headline from one of my posts.



The text in the brackets lets readers know that my post is up-to-date.

Create Captivating Introductions

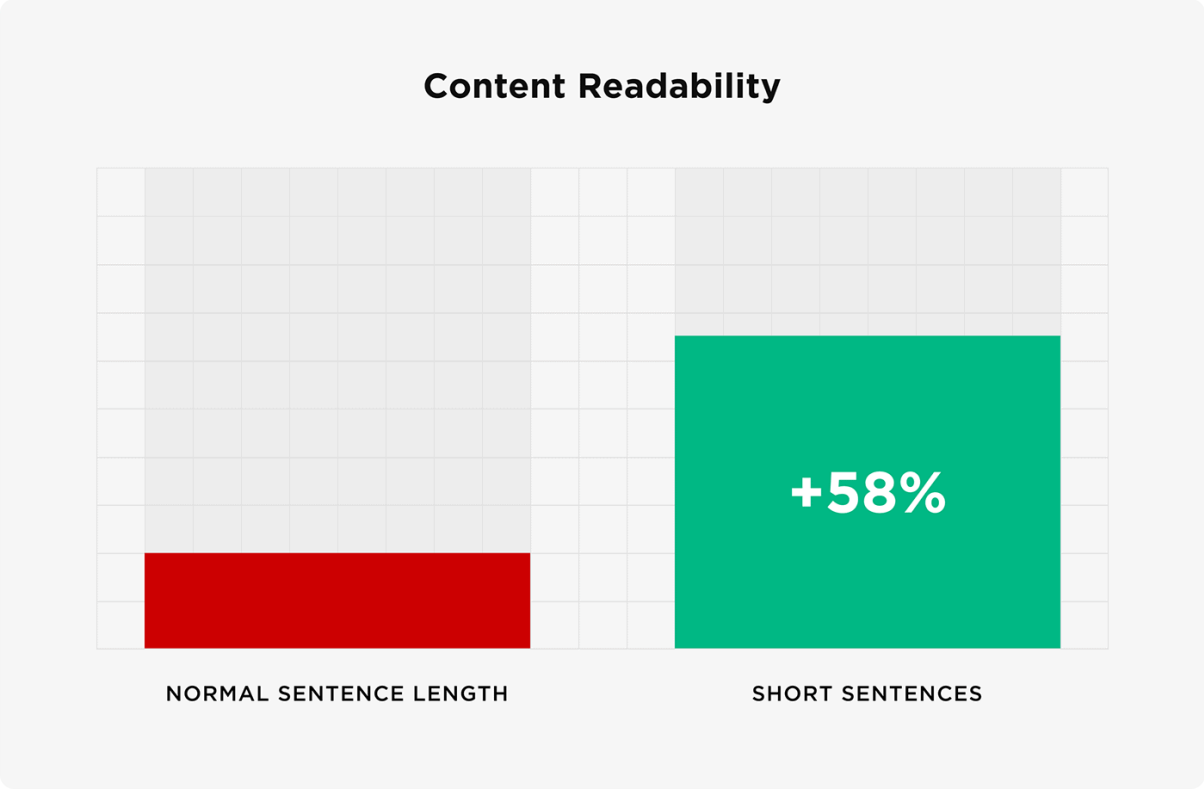
If you want to create a viral post, it's easy to overlook your introduction.

That said: people only read about 28% of a blog post. So if you want your post to go viral, you need to hook readers **fast**.

This means your intro should be compelling and interesting.

Besides that, you might also want to try using short sentences.

Dr. John Morkes found that short sentences boosted content readability by 58%.



Here’s an example of an intro that uses short sentences.

Today I’m going to show you how to write a blog post that gets:

Hundreds of comments.

Thousands of social shares.

And first page Google rankings.

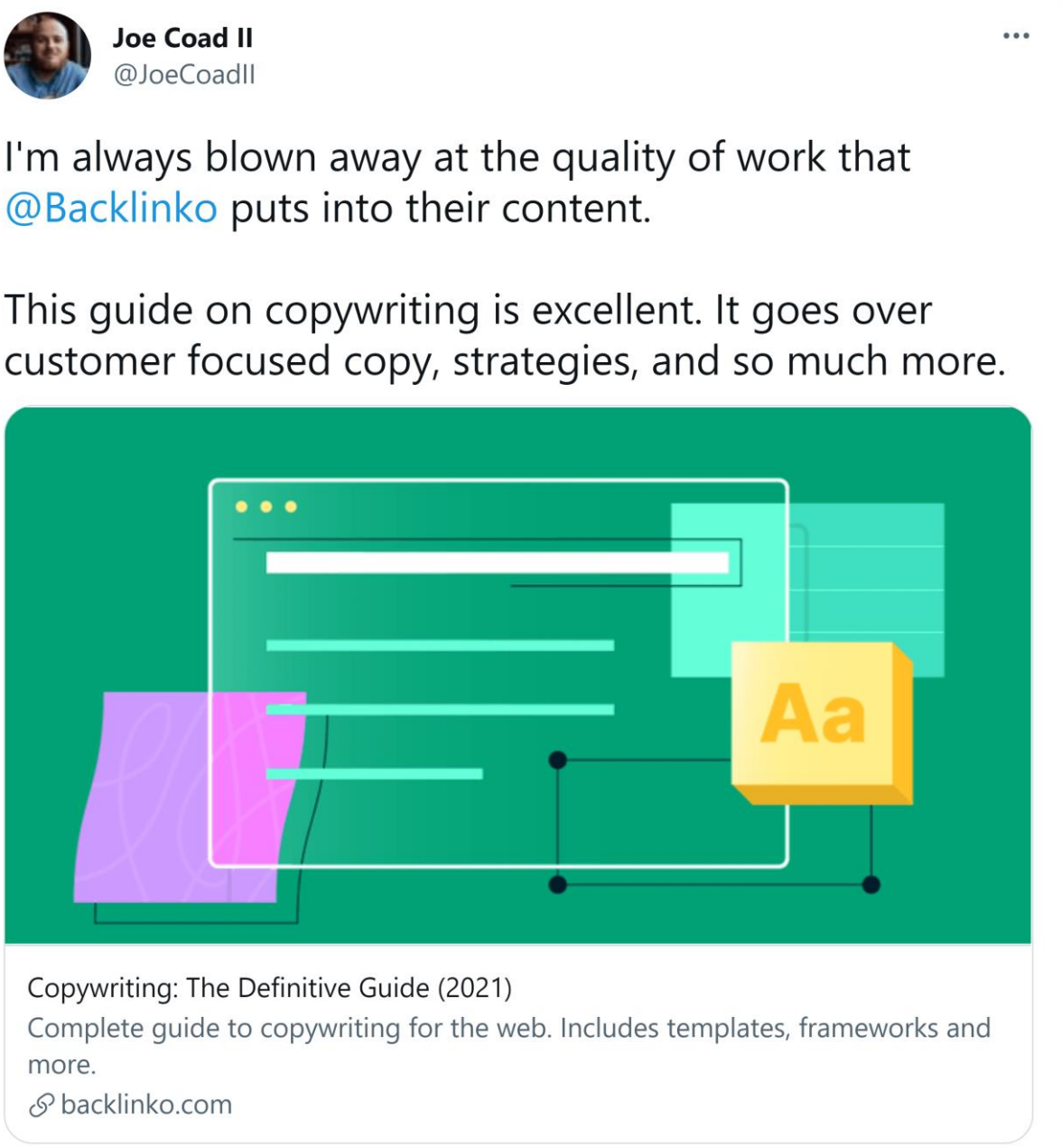
Let’s dive right in.

Use Colorful Visuals

Images makes your content much more compelling.

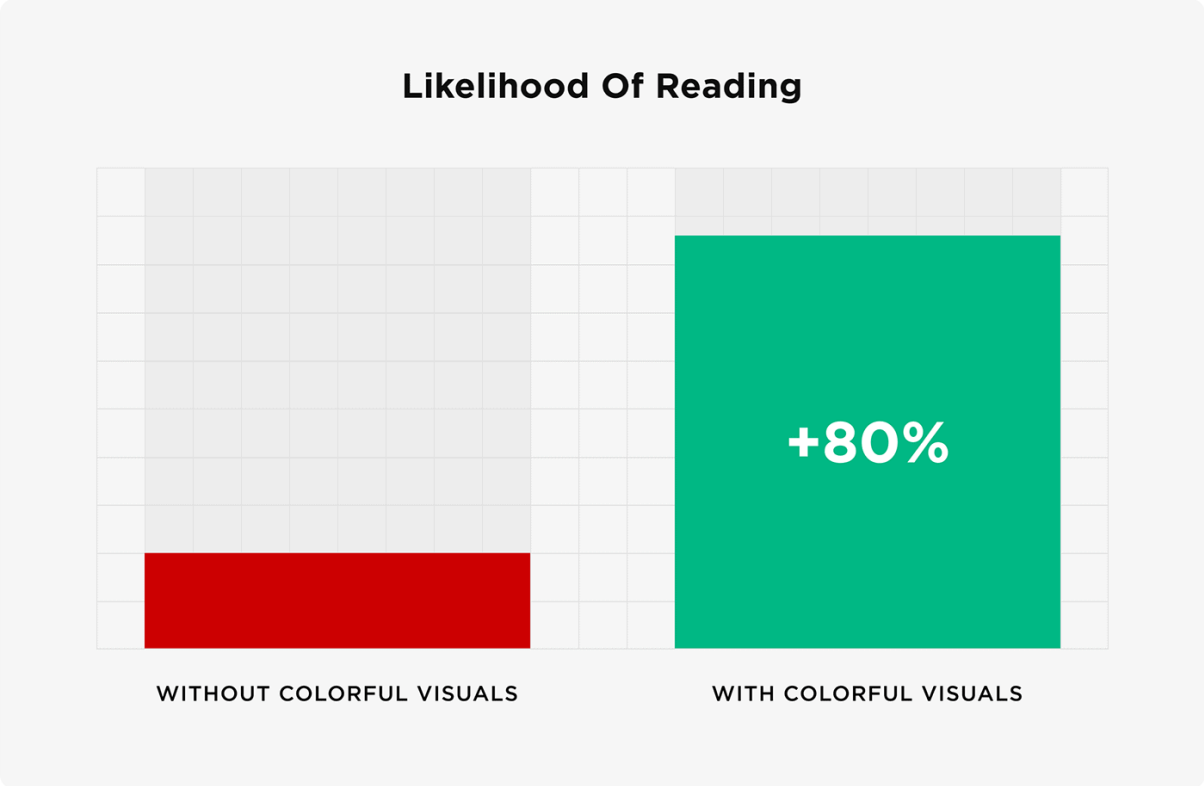
(Especially compared to a blog post that's 100% text.)

Plus, cool-looking visuals will end up in Tweets and Facebook posts… which can help your content go viral.



There's evidence to back this up.

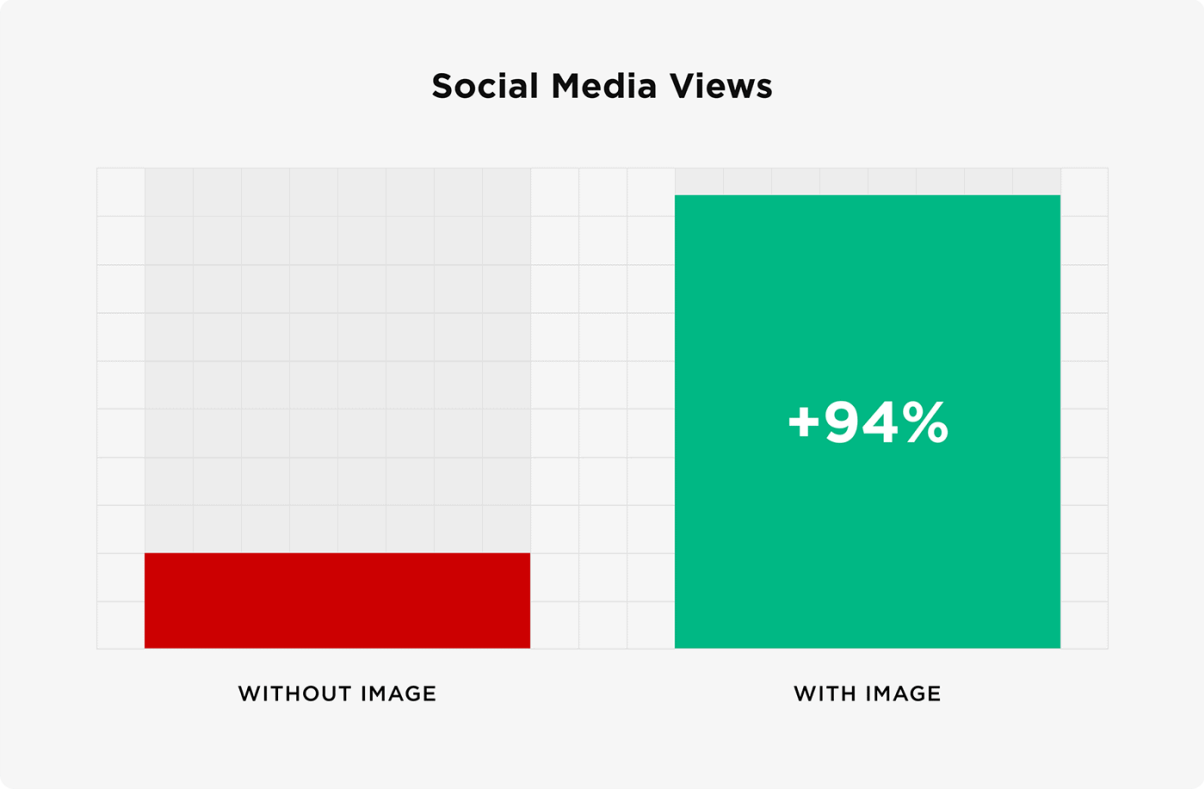
Xerox found that colorful visuals made people 80% more likely to read a document.



What if colorful images don’t make sense for your post?

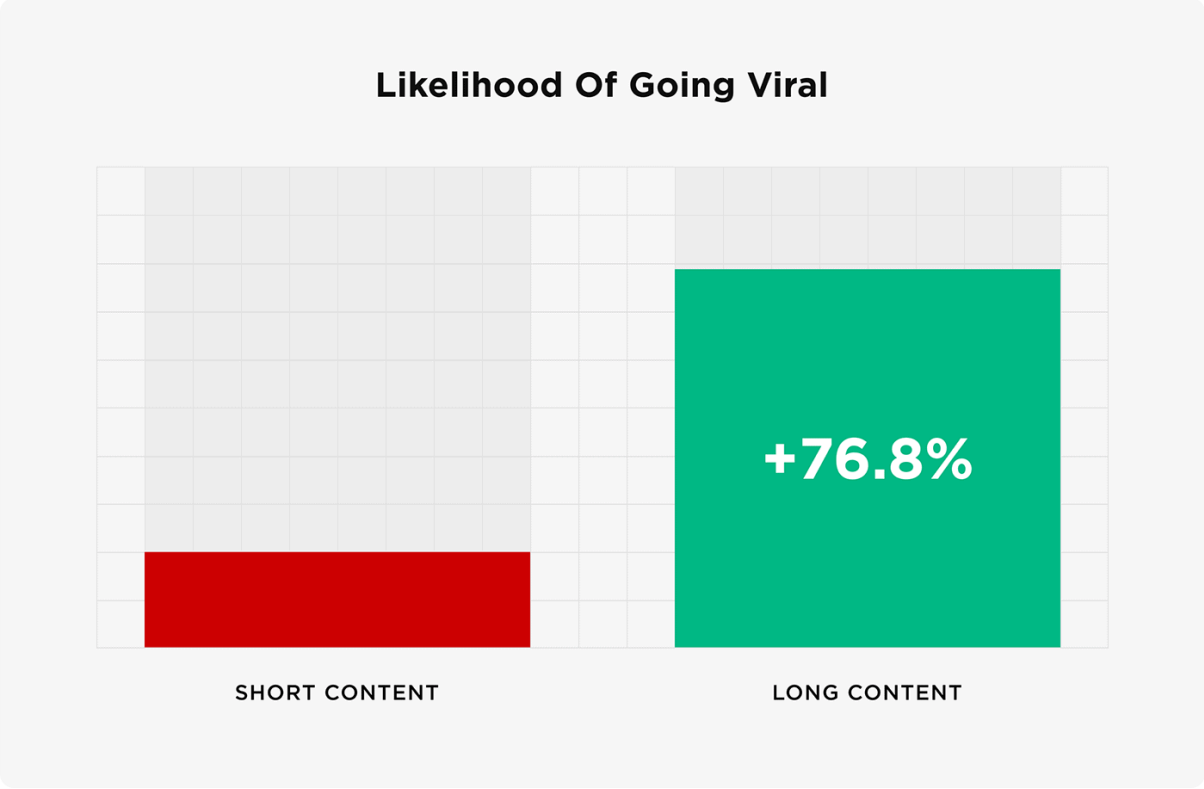
No worries. Just make sure to include something visual.

Skyword research found that text content with at least one image generated 94% more views on social media.



Experiment With Long-Form Content

In a study of virality, Professor Dr. Jonah Berger found that longer content was 76.8% more likely to go viral compared to short content.



There’s no magical length that will make your content go viral. But at least according to this research, longer content can increase your odds.

Set a Featured Image

Social shares with images get 150% more retweets on Twitter and 53% more Likes on Facebook.

This is why a “Featured Image” can help you create viral content.

A Featured Image is an image that automatically appears when people share your content on Facebook, LinkedIn and other social media websites.

For example, we set this as the Featured Image for this piece of content.

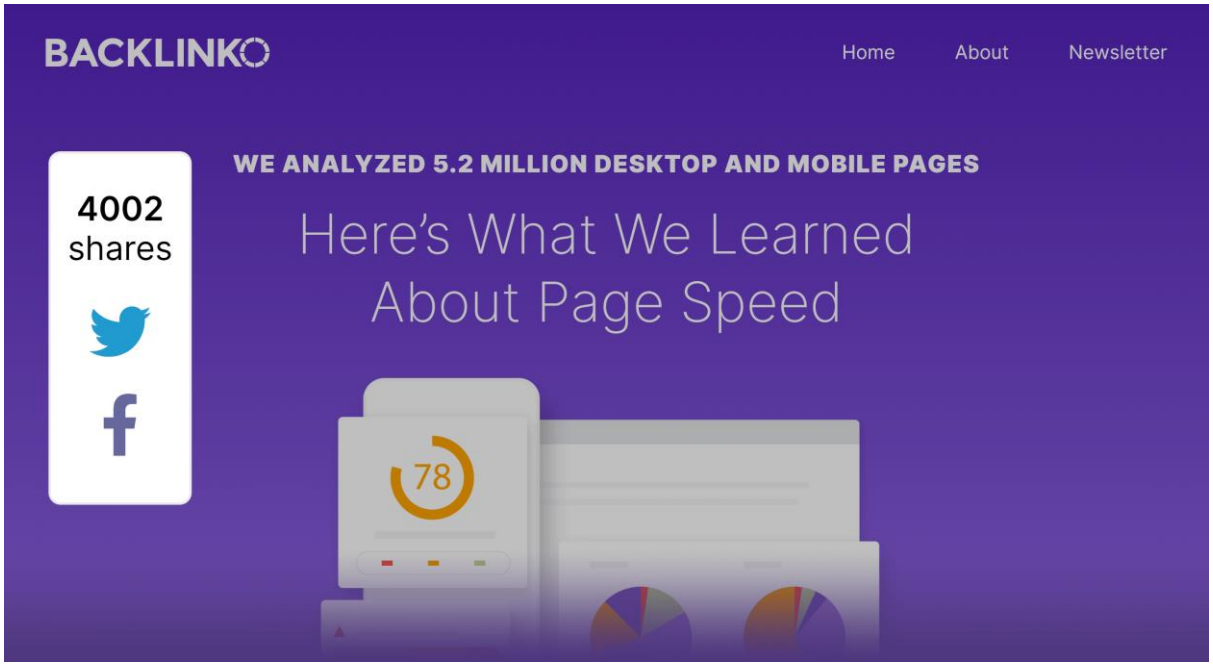
And whenever someone shares it, that image shows up underneath the post.

Place Share Buttons Above The Fold

A Google study found that elements above the fold are seen by 58% more people than elements that are further down the page.

This is why you want to place your social sharing buttons high up on your page.

Here's an example:



Publish Emotionally-Charged Content

A study published in the Journal of Marketing Research found content that elicits the emotions "awe", "surprise" or "anger" was 28% more likely to go viral. This applies to text content (like a blog post). But also works if your goal is to create a viral video.

The format isn't super important.

The important thing is that your content elicits an emotional response. That's one of the keys to creating shareable content.

Promote To Influencers

Sure, you should write content for your target audience.

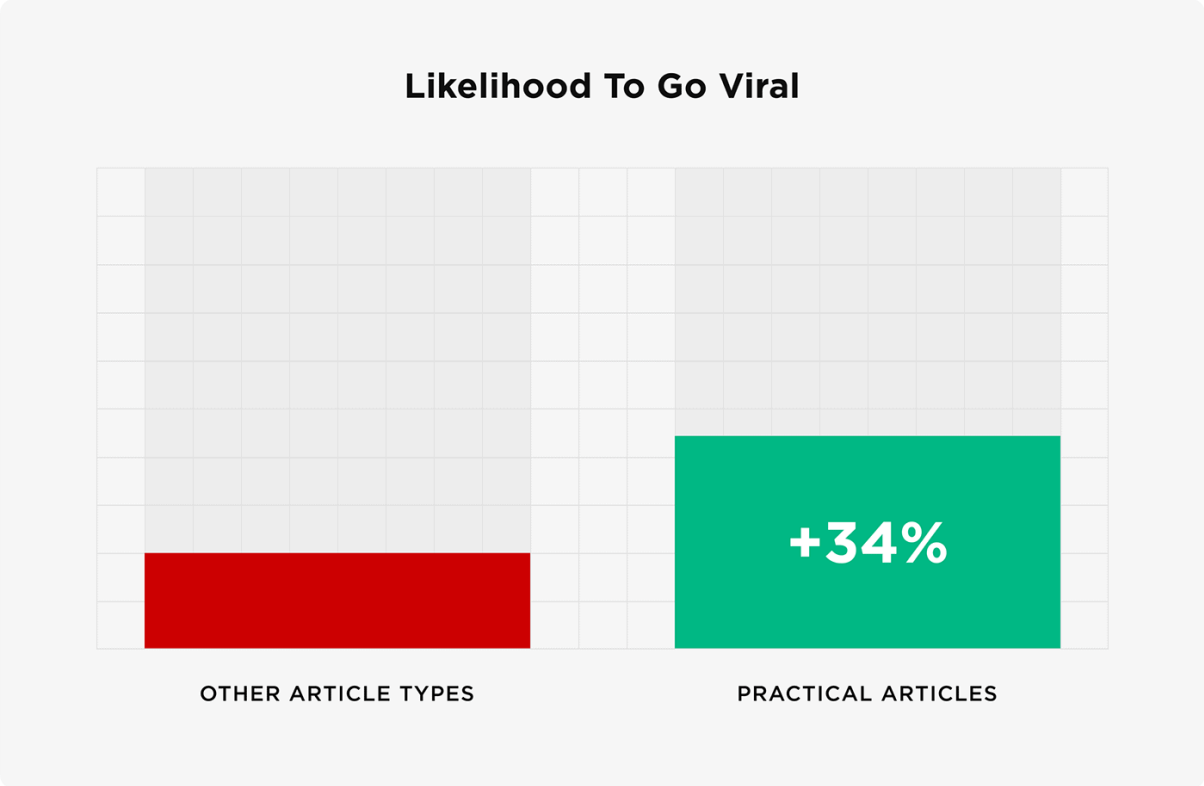
That's content marketing 101.

But don't forget to mention to influential bloggers in your post (and let them know about it).

A Columbia University study found that for your content to go viral, influencer shares were"critical". That's because these folks will share your content on social networks like Facebook, Twitter and YouTube… increasing the odds that you go viral.

Publish Practical Content

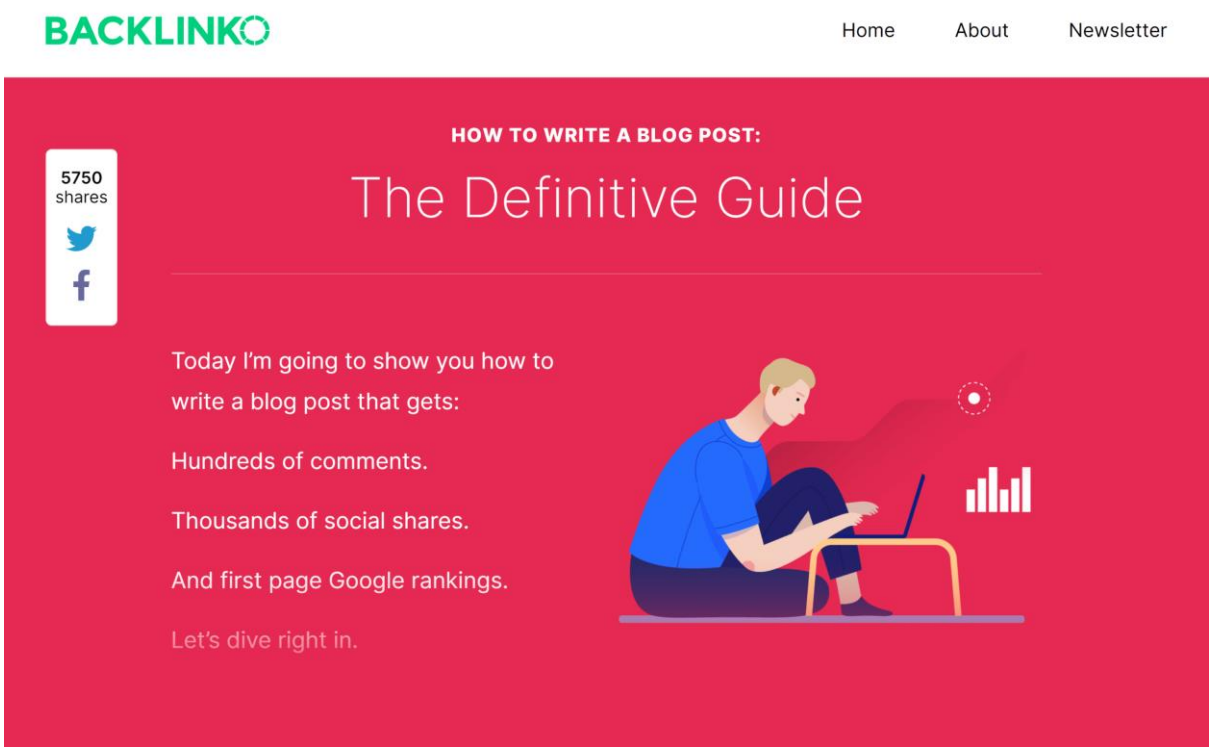
Dr. Jonah Berger found that highly-practical articles are 34% more likely to go viral.



So if you don't want to create controversial or emotionally charged content, consider practical content, like recipes and how-to guides.

When done well, practical content has a decent chance of going viral too.

For example, some time ago we published a guide to writing a blog post.



There wasn't anything super controversial or emotional in the guide. But it was super practical.

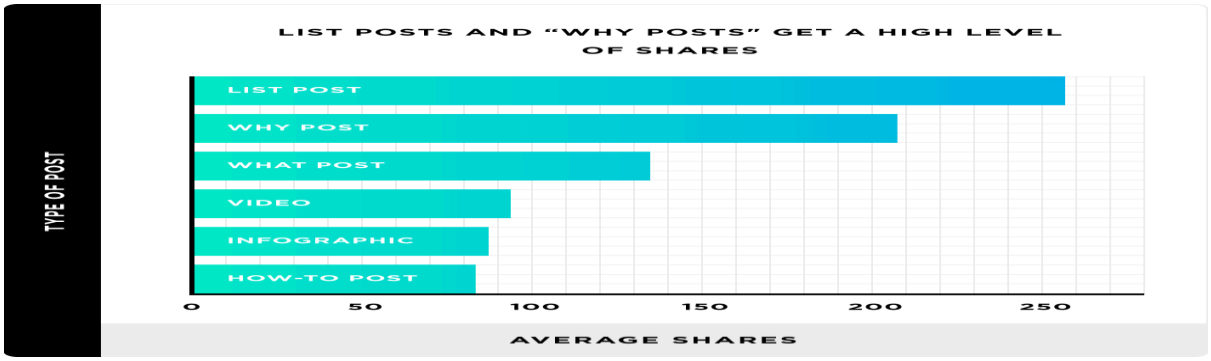
And all of the actionable tips in our guide helped it rack up 6346 shares.

Focus On List Posts and Why Posts

Are there types of content that get shared more often?

Yes.

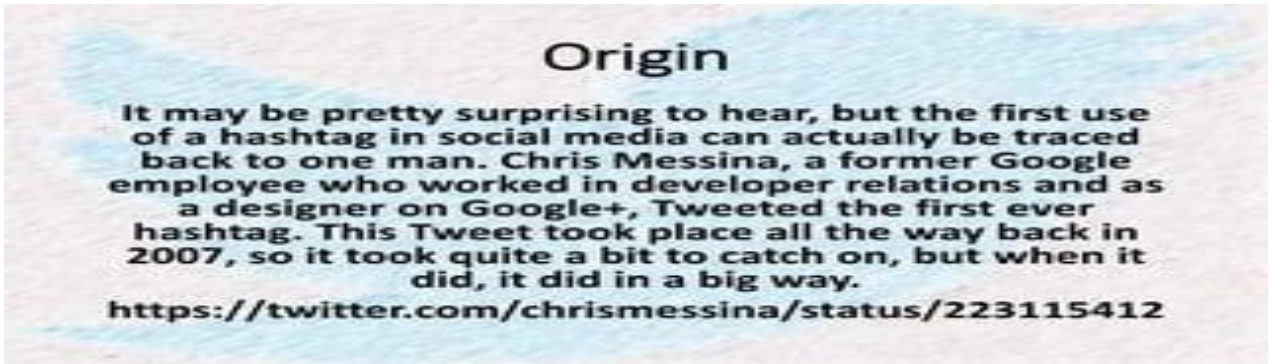
List posts and why posts get more shares than videos, infographics and how-to posts.

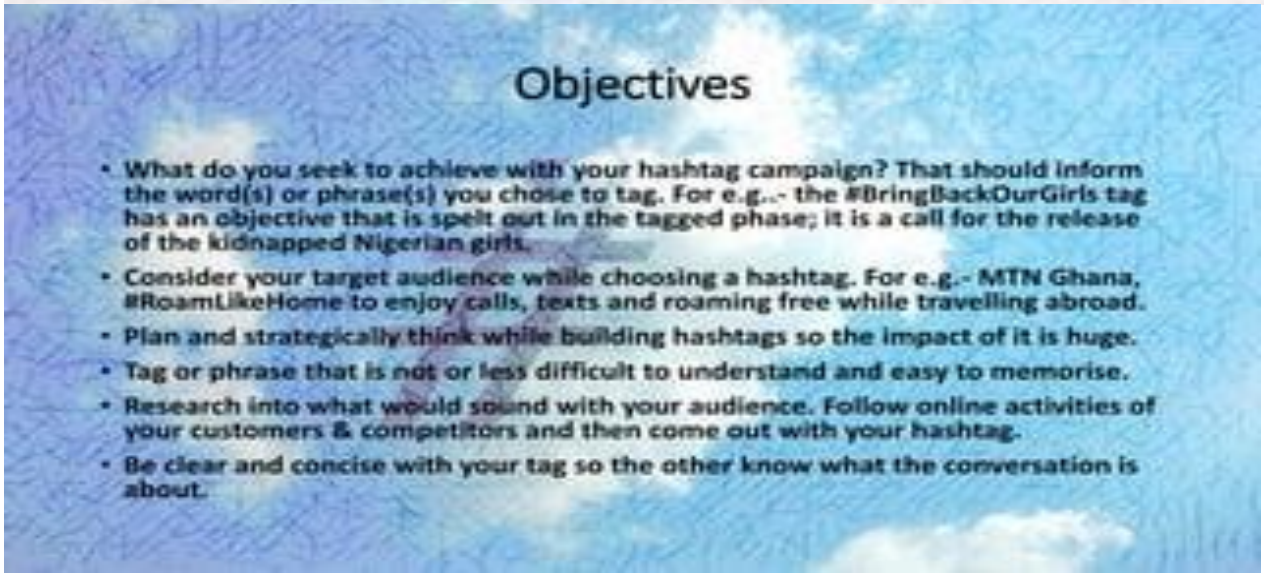


The downside is that these content formats don't get as many backlinks. So they're great for viral content campaigns… but not for SEO.

Hashtags

#Hashtag – The New Social media Trend- a Word or phrase preceded by hash mark(#) ,used within a message to identify a keyword or topic of interest and facilitate a serch for it.





How to use hashtags?

Using a hashtag in a social post is as simple as adding the '#' sign before a single word or phrase without spaces or punctuation (numbers are okay).

- Don't string too many words together with a single hashtag.
- If you tweet with a hashtag on a public account, anyone who does a search for that hashtag may find your tweet.
- Don't #again #with #hashtags. Don't over-tag a single tweet.
- Use hashtags only on tweets relevant to the topic.

Creating your own Hashtags

Creating your own hashtag can be a powerful thing. If you do it right, and have a lot of luck on your side, your hashtag will start trending among your circle of followers. Then, whenever someone sees that hashtag they'll be reminded of your brand.

The key is to creating a hashtag that doesn't leave you vulnerable is to write it free of ambiguity. It's important to completely guide how you want the conversation to go, otherwise you're at the mercy of the internet.

Advertising of Trending Hashtags

Trending hashtags states popular of all of them. You have probably heard, people talking about "what's trending new" means hashtags most talked about nowadays.

Instead of creating your own hashtags, you have the opportunity to craft Tweets based around trending hashtags in hopes of gaining visibility from users searching that trend. The absolute key thing to remember here is relevance. There are times when a brand attempts to force itself onto users through trending topics when it just doesn't make sense. It doesn't make for a good experience to be seen as an irrelevant ad.

Social Network support Hashtags

Renowned networks use Hashtags are-

Twitter- The network that brought us the hashtag is the most popular site to use it on. Just scrolling through my own feed I see that more than half of the tweets contain a hashtag.

Facebook- Clicking a hashtag on Facebook will bring you to a separate page with posts that are visible to you based on the various users' privacy settings.

Instagram- Hashtagging on Instagram is great if you want to see photos similar to the ones that you've taken.

Google+- Google+ uses hashtags similar to the other sites, but with one main difference. Google+ will add hashtags to content if they think that it is a relevant and popular keyword.

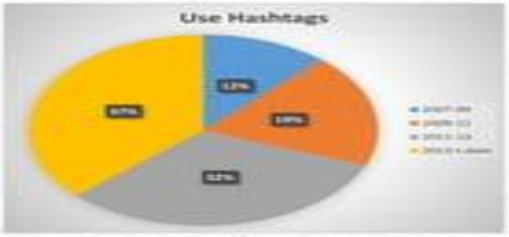
And many more like- YouTube, Tumblr, Pinterest, etc.

Are Hashtags here to stay?

Seeing as how they've been integrated into most of the popular social media platforms, and social media has entered almost every facet of our lives, the answer is yes.

Though they've become stigmatized in our culture, hashtags actually do play a vital role on social media when used within reason.

This is the graphical representation of sample space using Hashtags→



How Hashtags are useful to any Business?

- **Brand Hashtags-** They are the company name/company title. Make a brand hashtag that is Unique, Defines your business, ask people to quote them to make your brand popular.
- **Campaign Hashtags-** It is built to capture a large market. It is use to promote and advertise your company portfolio for marketing and sales.
- **Trending Hashtags-** They are the popular of all .By using a trending tag in your content update, you can potentially get your message seen to a massive audience. Eg.- OREO, one of the first brands to tweet about the trending hashtags like #SuperBowl and #blackout.
- **Content Hashtags-** These are the common hashtags reflected to your post content. They improve the SEO of your posts. They get your updates seen by your consumers who are searching for it. Here are a categories of Content Hashtags - 1. Product Hashtags, 2. Lifestyle Hashtags, 3. Event Hashtags and 4. Location Hashtags.

Competitive Brands Hashtags

NOKIA - #ConnectedCar, #LumiaLove, #ShotOnMyLumia, etc.

SAMSUNG - #GalaxyApp, #InGalaxy, etc.

SONY - #XperiaLounge, etc.

MOTOROLA - #MotoG, #MotoX, etc.

About GiONEE

A brand that's truly international

Gionee Communication Equipment Co. Ltd was founded on September 2002 by Liu Li Rong. It is a high tech enterprise that focuses on the R&D, production and sales of cellular mobile devices. In 2005, Gionee obtained the GSM and CDMA mobile phone production license.

Gionee's Headquarter, Shenzhen China, currently employs over 1500 employees with the average demographic less than 30 years old. Our management team advocates for a scientific and standardized enterprise management mode, with a strong sense of innovation. The constant pursuit for professionalism and innovation is the foundation of sustainable development at Gionee.

R&D Centres are set up in Shenzhen, Shanghai, Hangzhou and other places. In 2006, the first phase of the project had a total investment of more than 1Billion RMB and covers an area of 500 acres of the Gionee Industrial Park.

Gionee have launched around 29 phones in India.

Importance of Hashtags to GiONEE

- **Communication among users and the Gionee team would get simplified.**
- **Helping is building the brand name in public.**
- **Impression on social network on the Gionee products would increase.**
- **Team would try to build up the technology on the needs and demands of the public with the reviews or comments they will get on their defined and created Hashtag.**
- **Target a particular segment of market. Keeping them in mind, develop a product. Hashtags plays an important role in identifying a target market.**
- **Increase in the market share of the company.**

Social Network support Hashtags

Renowned networks use Hashtags are-

Twitter- The network that brought us the hashtag is the most popular site to use it on. Just scrolling through my own feed I see that more than half of the tweets contain a hashtag.

Facebook- Clicking a hashtag on Facebook will bring you to a separate page with posts that are visible to you based on the various users' privacy settings.

Instagram- Hashtagging on Instagram is great if you want to see photos similar to the ones that you've taken.

Google+- Google+ uses hashtags similar to the other sites, but with one main difference. Google+ will add hashtags to content if they think that it is a relevant and popular keyword.

And many more like- YouTube, Tumblr, Pinterest, etc.

Social Media Marketing for Businesses

Social media marketing is a powerful way for businesses of all sizes to reach prospects and customers. People discover, learn about, follow, and shop from brands on social media, so if you're not on platforms like Facebook, Instagram, and LinkedIn, you're missing out! Great marketing on social media can bring remarkable success to your business, creating devoted brand advocates and even driving leads and sales.

In this complete guide to social media marketing, you're going to learn:

- What social media marketing is, with benefits, stats, and tips.
- How to build a social media marketing strategy and a plan to carry it out.
- The seven best social media marketing platforms and how to use them

What is social media marketing? Social media marketing is a form of digital marketing that leverages the power of popular social media networks to achieve your marketing and branding goals. But it's not just about creating business accounts and posting when you feel like it. Social media marketing requires an evolving strategy with measurable goals and includes:

- Maintaining and optimizing your profiles.

- Posting pictures, videos, stories, and live videos that represent your brand and attract a relevant audience.
- Responding to comments, shares, and likes and monitoring your reputation.
- Following and engaging with followers, customers, and influencers to build a community around your brand.

Social media marketing also includes paid social media advertising, where you can pay to have your business appear in front of large volumes of highly targeted users.

Benefits of social media marketing

With such widespread usage and versatility, social media is one of the most effective free channels for marketing your business today. Here are some of the specific benefits of social media marketing:

- **Humanize your business:** Social media enables you to turn your business into an active participant in your market. Your profile, posts, and interactions with users form an approachable persona that your audience can familiarize and connect with, and come to trust.
- **Drive traffic:** Between the link in your profile, blog post links in your posts, and your ads, social media is a top channel for increasing traffic to your website where you can convert visitors into customers. Plus, social signals are an indirect SEO factor.
- **Generate leads and customers:** You can also generate leads and conversions directly on these platforms, through features like Instagram/Facebook shops, direct messaging, call to action buttons on profiles, and appointment booking capabilities.

- **Increase brand awareness:** The visual nature of social media platforms allows you to build your visual identity across vast audiences and improve brand awareness. And better brand awareness means better results with all your other campaigns.
- **Build relationships:** These platforms open up both direct and indirect lines of communication with your followers through which you can network, gather feedback, hold discussions, and connect directly with individuals.

- The bigger and more engaged your audience is on social media networks, the easier it will be for you to achieve your marketing goals.

-

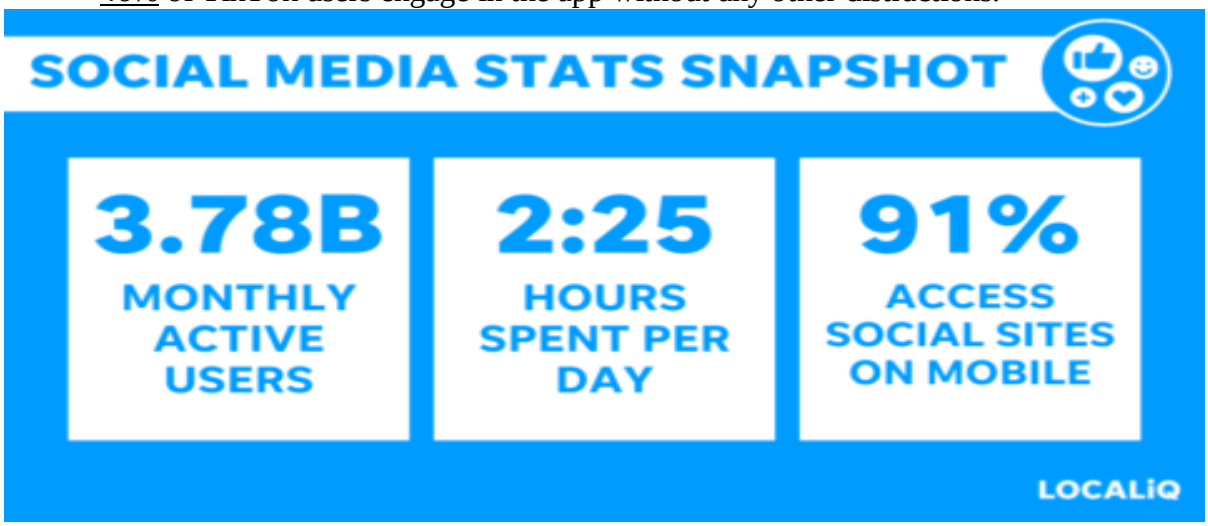
Social media marketing statistics

With regard to the benefits above, don't just take our word for it. Let's take a look at some social media marketing statistics that prove its power:

- The average US adult spends 2.25 hours on social media every day.

- Over 70% of people who have a positive experience with a business on social media will recommend that business to their networks.
- Facebook users click on 12 Facebook ads on average every month.
- 81% of people use Instagram to research products and services.

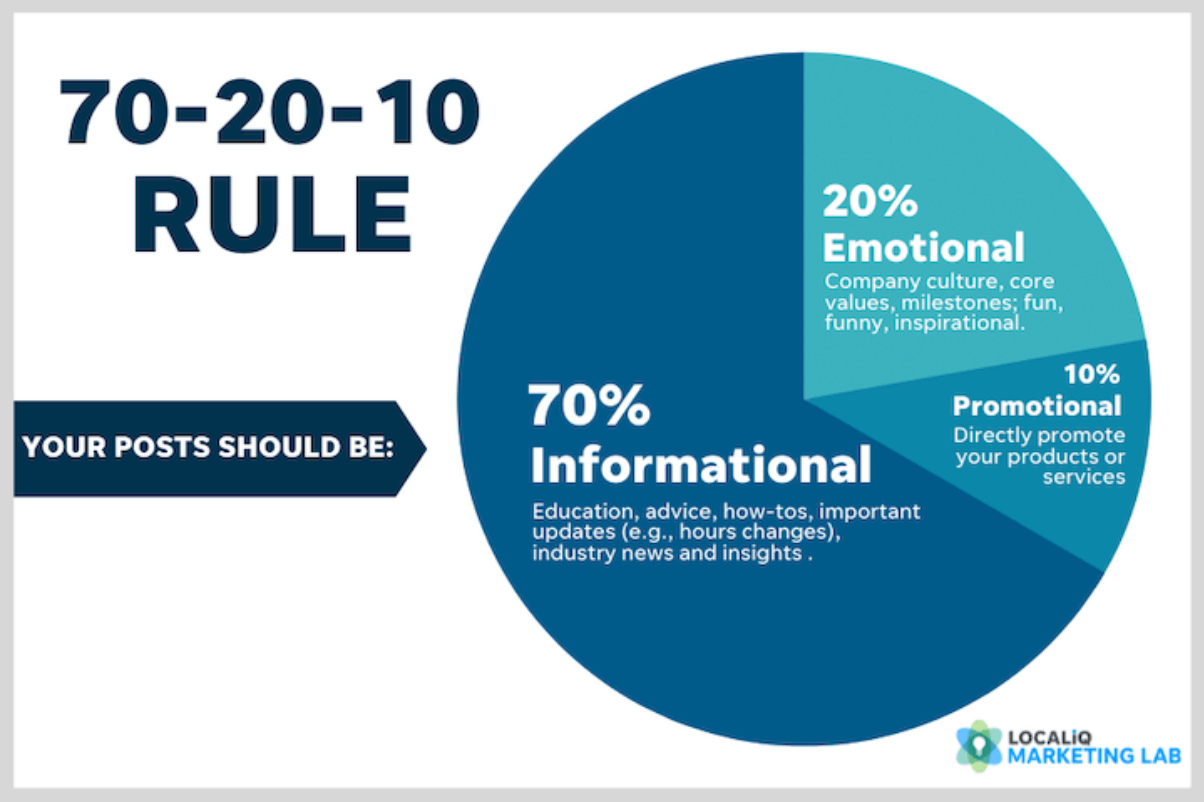
- Nearly 80% of Twitter users feel more positive about a business when they get a response to their tweet.
- 4 out of 5 people on LinkedIn drive business decisions.
- 46% of TikTok users engage in the app without any other distractions.



The essentials of a successful social media marketing strategy

A successful social media marketing strategy will look different for every business, but here are the things they will all have in common:

- **Knowledge of your audience:** What platforms they use, when they go on them and why, what content they like, who else they're following, and more.
- **Brand identity:** What is the message you want to convey to your audience? How do you want them to feel when viewing your content?
- **Content strategy:** While there is a level of spontaneity on social, you'll need a structured content strategy to be able to have a consistent voice and produce quality content regularly.
- **Analytics:** Quantifiable insights will inform your strategy, including who you're reaching, the right content to share, the best times to post, and more.
- **Regular activity:** Social media is a real-time platform. If you want to use it to grow your business, you need to post regularly, stay on top of engagements with your business, engage back, keep up with trends, and maintain accurate profiles.
- **Inbound approach:** Don't use social media to pitch your business. Focus on adding value through useful and interesting content and building up those around you. This, in turn, will organically promote your business and others will promote it for you.



Creating your social media marketing plan

Now that you know the essentials of a social media marketing strategy, it's time to put it into action. Your social media marketing plan is the roadmap to carrying out your strategy. It puts structure around your efforts so you can measure your success and make sure you're spending your resources wisely. Here's how to create your social media marketing plan:

1. **Choose your platforms:** Choose based on your target audience, platforms popular for your industry, as well as your bandwidth. Only take on the number of platforms you can actively keep up with. You can always start with one and then add on more slowly as you get the hang of them.
2. **Set goals and objectives:** These should be simple and task-like to start, like post once a day for a month, get your profiles set up, or do a competitive analysis. Once you get into a rhythm and gather insights, you'll be able to set more specific and strategic goals like increase your following by X% or publish X [content types you've found your audience likes] per month.
3. **Report and adjust regularly:** Use each platform's analytics to identify which posts generate the most engagement, whether you're getting more followers, and to see your audience demographics. Harness and scale up what works and nix what doesn't.

Social media marketing tips

Ready to get started with marketing on social media? Here are a few social media marketing tips to kick off your social media campaigns.

Create diverse content

Consistent with other areas of online marketing, content reigns supreme when it comes to social media marketing. Make sure you post regularly and offer truly valuable information that your ideal customers will find helpful and interesting. This includes:

- How-tos, quick tips
- Local and industry news
- Data and insights
- Polls, questions, contests
- Updates and announcements

It also means making use of the variety of formats social media offers, including images, videos, stories, live streams, online stores, and more.

Stay consistent

Using social media for marketing enables your business to project your brand image across a variety of different social media platforms. While each platform has its own unique environment and voice, your business's core identity, whether it's friendly, fun, or trustworthy, should stay consistent.

Don't just post—participate

In other words, don't just log in once a month to schedule out all your posts. Social media channels are communities. You need to pay attention to who's engaging with your content and engage back—respond to comments, like, share and comment on their posts, run live streams, post polls and real-time questions to spark discussions, and repost others' content.

Use content creation tools

Don't let anyone tell you that Instagram is the most visual social media platform. They all are! If you want to stand out in a person's feed, you need to accompany your posts with attractive visuals—photos, illustrations, text turned into art. Content creation tools like Freepik and Canva have templates and features that allow you to quickly create visuals that look professional, have your logo on them, and are consistent with your brand.

Repurpose, repost, recycle

Social media is a crowded place, so if you want to gain traction with your audience, you need to post great content regularly. The secret to doing this? The three Rs:

- **Repurpose:** Create a Facebook post from a customer review, splice up a blog post into a series of Tweets, distil a case study down into a customer spotlight on Instagram; turn a webinar deck into a carousel post on LinkedIn. The possibilities are endless.
- **Repost:** To be done in moderation, but a great way to fill gaps in your content calendar. Repost on Instagram and retweet user-generated and influencer content. You can also curate content from authoritative sources and share those links in your posts.
- **Recycle:** Post your TikTok videos and Instagram Reels to YouTube; re-share your top-performing blog posts every month to get in front of new followers; add your Facebook Live recordings to your YouTube channel.

Curate your own feed

We're always looking for ways to show up in others' feeds, but we forget that there is value to be derived from our own. Follow your competitors so you can keep tabs on them, get ideas you can adapt to your own strategy, and identify gaps you can fill. Follow influencers to stay on top of trends and educate yourself. Follow brands that share your values or that have great content strategies for inspiration and outside the box ideas.

Measure success with analytics

You can't determine the success of your social media marketing strategies without tracking data. Google Analytics can be used as a great social media marketing tool that will help you measure your most triumphant social media marketing techniques, as well as determine which strategies are better off abandoned. Attach tracking tags to your social media marketing campaigns so that you can properly monitor them. And be sure to use the analytics within each social platform for even more insight into which of your social content is performing best with your audience.

Try paid social

Among the many reasons to advertise on social media is that it is a highly cost-effective way to expand your reach. If you play your cards right, you can get your content and offers in front of a huge audience at a very low cost. Most social media platforms offer incredibly granular targeting capabilities, allowing you to focus your budget on exactly the types of people that are most likely to be interested in your business. Below are some tips and resources for getting started with paid social media marketing:

- Facebook ads
- Pinterest ads
- Instagram ads

The best social media marketing platforms for business

The best social media marketing platforms for business include Facebook, YouTube, Instagram, LinkedIn, Twitter, TikTok, and Snapchat. Different social media marketing sites require different approaches, so here's a brief overview on each one—its user base, main vibes, pros, cons, and content types.

Facebook

Facebook is the largest social media platform globally as well as one of the biggest local business directories. People of a diverse range of age groups use it to communicate with friends and family, participate in groups and forums, find and visit businesses near them, and follow brands. Facebook is a great social media marketing platform to:

- Build relationships with current customers
- Announce hours changes, events, and milestones
- Hold discussions and live streams

Market to baby boomers
Organic reach on Facebook is limited, so if you're looking to generate leads or find new audiences, Facebook advertising is your best bet.

YouTube

You may not think of YouTube as a social media marketing channel, but it fits the bill: you can post videos to your channel; share, comment on, and like other videos, and follow other accounts you like. Plus, you have a curated feed in your homepage with recommended videos. The key to social media marketing on YouTube is not to try to "go viral," but to add value. It's best for:

- Tutorials, how-tos, and explainer videos
- Shoppable YouTube live streams
- Advertising (video ads and display ads on the platform)
- SEO (video is dominating the "how to" SER

Instagram

Though it came onto the scene years after LinkedIn and Twitter, Instagram quickly surpassed those platforms and reached one billion monthly active users in 2018. It's popular for its diverse content formats, including Feed posts, Stories, Lives, Reels, and IGTV. People use Instagram to follow influencers and brands they buy from and who support their personal values. Create your Instagram bio and then use it for:

- Social shopping
- Influencer marketing

- User-generated content
- Company culture

The cost of Instagram ads is generally higher than on Facebook, but the good news is that organic reach is also higher.

LinkedIn

LinkedIn may be a professional network, but it's also an inspiring community that celebrates leadership, learning, and core values. So in addition to using it to network, find prospects, and share industry insights, it's also a great place to express your company culture and build your personal brand in parallel with your business brand. There are tons of LinkedIn company page features to take advantage of, so take care when building your page. LinkedIn is a great platform to:

- Attract top talent
- Network with partners, peers, and customers
- Share company milestones and culture
- Post industry news and insights

Twitter

Twitter is a beautifully tangled network of quick thoughts, useful tidbits, and energized discussions. You should be regularly active on every social media platform, but it's especially important here. Many people use Twitter to get news, follow brands, and get customer service. Be sure to retweet when a customer has something nice to say about you, and don't forget to answer people's questions when possible. For effective social media marketing on Twitter, you may want to:

- Follow influencers to keep up with news and trends.
- Share a story through a series of Tweets in one thread.
- Make yourself available for customer service and FAQs.

Snapchat

Snapchat isn't just for teens. Its largest age group (75%) ranges from 13-34 and with Snap Maps, geofilters, and its partnership with Gannett, it's more locally-focused than you might think. While you can't build relationships on the platform, you can build an audience through fun images and short videos. Use Snapchat for:

- Location-based marketing

- App marketing
- Feel-good content

TikTok

TikTok is the fastest growing social media platform of all time, taking only five years to reach one billion monthly active users. While it's known for dancing, there are countless popular categories on the platform that continue to grow. Businesses are finding ways to use it as a marketing channel, but just remember, the primary reason people use TikTok is for entertainment, so make sure your videos align with that. Use TikTok to:

- Participate in trending challenges
- Post funny and inspiring videos
- Be relatable

Social media marketing services

As free and easy as each platform may be, a solid social media marketing strategy requires multiple platforms and often a mix of organic and paid methods. This can be resource-heavy, and while it's a good problem to have, the more you grow your audience using social media, the harder it will be to keep up. Social media marketing services come in all kinds of shapes and sizes to help businesses get the most out of social media. For example:

- **Social media management software:** Social media management platforms like HootSuite and Sprout Social use proprietary technology to help more experienced social media marketers streamline their processes and get advanced analytics.
- **Social media marketing agencies:** Some agencies specialize in social media marketing only, like Akvertise or even just paid social advertising only.
- **Digital marketing agencies:** Just as one platform doesn't do it for social media marketing, one channel doesn't do it for overall marketing. Digital marketing agencies can help you to incorporate social media marketing into your broader strategy that includes email, website, SEO, and more.
- **Hybrid services:** Some offer a mix of the above. For example, LOCALiQ's social advertising offerings use proprietary technology to manage your strategy and allow you to focus on social alone or as part of a broader plan.

Start prioritizing your social media marketing strategy

Using social media in marketing does more than improve site traffic and increase your reach. It turns your business into a personality that your audience can communicate and connect with on a deeper level.

Regardless of which platforms you use or how you use them, the most important thing to remember is that social media is not a platform to pitch your business. It's a community for you to express your personality, demonstrate your values, share useful information, and build up those around you. With people naturally following you and promoting your content, there

will be no need for pitching. And with this approach, you'll achieve not just your business goals but all of the other intangibles that translate to gratification and fulfillment.

Common social media privacy issues

With the large amount of data on user social media accounts, scammers can find enough information to spy on users, steal identities and attempt scams. Data protection issues and loopholes in privacy controls can put user information at risk when using social media. Other social media privacy issues include the following.

1. Data mining for identity theft

Scammers do not need a great deal of information to steal someone's identity. They can start with publicly available information on social media to help target victims. For example, scammers can gather usernames, addresses, email addresses and phone numbers to target users with phishing scams.

Even with an email address or phone number, a scammer can find more information, such as leaked passwords, Social Security numbers and credit card numbers.

2. Privacy setting loopholes

Social media accounts may not be as private as users think. For example, if a user shared something with a friend and they reposted it, the friend's friends can also see the information. The original user's reposted information is now in front of a completely different audience.

Even closed groups may not be completely private because postings can be searchable, including any comments.

3. Location settings

Location app settings may still track user whereabouts. Even if someone turns off their location settings, there are other ways to target a device's location. The use of public Wi-Fi, cellphone towers and websites can also track user locations. Always check that the GPS location services are turned off, and browse through a VPN to avoid being tracked.

User location paired with personal information can provide accurate information to a user profile. Bad actors can also use this data to physically find users or digitally learn more about their habits.

4. Harassment and cyberbullying

Social media can be used for cyberbullying. Bad actors don't need to get into someone's account to send threatening messages or cause emotional distress. For example, children with social media accounts face backlash from classmates with inappropriate comments.

Doxxing -- a form of cyberbullying -- involves bad actors purposely sharing personal information about a person to cause harm, such as a person's address or phone number. They encourage others to harass this person.

5. False information

People can spread disinformation on social media quickly. Trolls also look to provoke other users into heated debates by manipulating emotions.

Most social media platforms have content moderation guidelines, but it may take time for posts to be flagged. Double-check information before sending or believing something on social media.

6. Malware and viruses

Social media platforms can be used to deliver malware, which can slow down a computer, attack users with ads and steal sensitive data. Cybercriminals take over the social media account and distribute malware to both the affected account and all the user's friends and contacts.

How to protect your information

Think twice when opening a new social media account because each platform adds an additional risk. Make sure the platform is safe and reliable before joining. When leaving a platform, make sure to delete the account.

Other ways to keep information safe include the following:

- **Use strong passwords.** Don't reuse passwords across multiple programs or websites. For help remembering sign-on credentials, use a password manager to store information securely.
- **Avoid public devices.** When using a shared device, be sure to log out when finished.

- **Don't overshare.** Avoid providing more details than necessary. Users shouldn't have to share addresses or date of birth on all platforms.
- **Disable geolocation data.** Disable sharing location information on apps in the privacy and security settings on the phone.
- **Don't click on suspicious links.** Even if the link appears to be from a friend, avoid clicking on links unless it's from a trusted source.
- **Use two-factor authentication.** Implementing two-factor authentication, such as a passcode and biometric recognition, adds another layer of security to the app.

Security issues in online social media

Below is the list of few security threats that we might face in social media accounts:

- Most social networking sites have information like Birthday or Email address. Hacker can hack your email account by using social information and can have access to all the information he/she wants. You don't need to hide all information. You just need to take the following precautions:
    - Always set strong passwords. Don't go for the easy passwords built using your Birthday or child's name etc. i.e., from the information that is easily accessible from the social media account.
    - Don't reveal too much information in a post. Be careful with what you post online. For example, if I write *"Happy Mother's Day Mumma Richa Sahani"*. Now you see one can guess an answer to one of my security question "What is your Mother's Maiden Name?". This how it works for the thieves to get information by just analyzing your posts. They get so much information that they can even compromise your account.
    - Don't reveal your location. Try to keep the location section either blank or set it to a false location.
    - Do not use social media accounts from untrusted devices and networks in hotels, cafés, hospitals etc.
    - Do not elect to remember passwords/passphrases for social media accounts when offered by web browsers.
- With the advent of Social Media like Twitter, there comes URL Shorteners in picture. Twitter allows a post to be maximum of 280 characters. Thus limiting the size and amount of information that can be shared. Shortened URL's can trick users into visiting harmful sites since full URL's are not visible. It is best to keep following points in mind before clicking on shortened URL to avoid being hacked.
    - Before clicking a link, place the cursor on the shortened URL. This will show the complete URL and will give you an idea about where the full URL actually points.
    - Check the shortened URL using the services that are available online like Sucuri to check whether the link is secure or not.
    - Use services like URL Void or MyWOT to check the safety status of the link.
- Avoid posting too much details online. Will you ever stand in the middle of the crowd and shout that you are going on a vacation to so and so place? So why you post all the

details of your trip on social media, with every second detail like *"Travelling to London, United Kingdom from Air India Business Lounge New Delhi".* You are clearly giving your house keys to burglars. Try to take following precautions while posting any information online:
    - Avoid posting specific travel plans and itinerary. Never mention exact date and time.
    - Never post photos during the trip. Try to post photos after your return home from the vacation.
    - Try to stay offline during vacation.
    - Use the highest privacy controls to let only selective groups like family, selected friends to view your status updates and photos.
- Have you ever wondered how we see a product on Flipkart and when we open another site, it will show the advertisement related to the product that we earlier searched on Flipkart. Every time we visit a website, it put invisible marker which we call Cookies in technical terms in our computer. Job of these cookies is to track the user activity as we navigate from one site to another. This is the reason we are able to see the advertisements of our interest on the new page that we open. Cookies are the major loophole in the entire secure scenario. Most sites provide a option to opt out of the tracking feature, but if you don't get that option, Please be careful to clear the cache and the cookies on your browser regularly.

The Pitfalls And Challenges of Social Networking

- Corporate and government entities are increasingly using social networking to facilitate communication and collaboration among individuals and groups, both internally and externally. While there are clear benefits to increasing communication, social networks also present a number of challenges, including the following:

- **Bandwidth and storage consumption.** Many social network members post pictures, music, videos, high-definition movies and other large files. Downloading and storing these files can cripple your infrastructure and make capacity planning virtually impossible.

- **Potential legal liability.** Students at Canterbury's University of Kent created a Facebook group named "For Those Who Hate the Little Fat Library Man," to harass a librarian they disliked. In the U.S., if employees were to use corporate IT resources for similar purposes, the company could be held responsible in any ensuing litigation.

- **Exposure to malware.** Social networks are designed to be open, with few restrictions on content or links. In most cases, security was not a primary design criterion. Thus, these networks are potential vehicles for introducing viruses, worms and spyware.

- **Decreased employee productivity.** Social networking for personal purposes can affect corporate productivity. A Goldman Sachs trader in the U.K. was spending four work hours a day on Facebook. When he was told to stop, he posted the warning e-mail and wrote, "It's a measure of how warped I've become that, not only am I surprisingly proud of this, but losing my job worries me far less than losing Facebook."

- Even when networking is used for business purposes, corporations may want to limit the number of networks employees use. Monitoring many networks can become incredibly time-consuming. Moreover, interfaces among current networks don't support robust information-sharing. Unfortunately, unless all interested parties use the same network, many benefits are lost. Consider designating specific networks for companywide communications.

- **Disclosure of personal information.** Companies regularly search MySpace, Classmates.com, LinkedIn and other social networking sites to glean information about potential hires and competitors, but postings should always be taken with a grain of salt.

- **Risk of leaking corporate secrets.** Companies often sanction social networking for the purpose of exchanging professional information. But take great care to protect corporate secrets. Definitions of secret may vary or be misunderstood, and critical information may inadvertently be revealed. Provide clear guidelines across the company, as well as to your suppliers and outsourcers.

- **Limited executive use.** Many articles on social networking claim that it will facilitate sales. Executive use of social networking is not widespread, however. Many executives already have substantial personal networks and rely less on new technological platforms for interaction. (This will undoubtedly change in the future, but networks have limited selling power today.)

- While social networking does offer many benefits, there are corporate costs and pitfalls to be considered. Organizations need to establish policies to address issues such as personal usage, business relevance, site restrictions and information confidentiality. Take time to thoroughly investigate and address these issues to maximize the effectiveness of social networking

Opportunities in social media

- here's a list of opportunities relating to social networks.
- 1. Data Mining/Research
- A main attribute of social networks is how much data people provide to them. On top of it, this data and the interaction of users on those networks. This is rich fodder for data mining. For example, researchers recently used Where's George, a website tracking dollar bills in the real world, to assess how disease spreads. Similarly, LinkedIn provides its users with demographic/geographic data about members of your social network.
- Traditional companies spend millions of dollars trying to understand the flow of people, flow of ideas (or memes) and how to exploit them. From Milgram's small world experiment to the success of "The Tipping Point" by Malcolm Gladwell, there has been a fairly large body of research in this area but, for what may be the first time in history, there is now a heavy trove of data that can be analyzed.
- 2. Problem Solving
- Sites like Google Answers are working on providing better answers to questions. Add-in some social network glue and one could be able to figure whether the person is a subject matter expert in the area he/she is answering the question about. For example, you might want to trust an individual with strong network ties in technology on

questions related to technology but might be a little more wary of answers that person would provide about medical care (and similarly, you might trust a doctor more about medical care than you would a computer geek). Social networks, when seen through the lens of expertise, can provide quick access to answers from subject matter experts in one area. It is impossible to know everything but you might have a friend of a friend of a friend who has the answer in a specific area you are researching.

- Similarly, social networks can provide a way to get social matter experts to connect and work collectively on difficult problems. When combined with digg-like features, social networks could become a way to speed up the vetting process on scientific publications by allowing a large set of peers to review articles and rank them according to value. This, in itself, could help humanity make radical moves forward in the area of scientific research.
- Take, for example, my friends at ACOR who have been thinking of developing, in partnership with the National Cancer Institute, a data-mining system that analyzes information about patients to identify potential root cause for different cancers. Here, we see social networks (in this case, via mailing lists that are finely targeted) potentially being useful to help advance science and hopefully discover some root causes for cancer. A set of tools to such granular community could help a scientist, for example, sent a questionnaire to a sub-segment of the population to test a hypothesis (eg. “let’s see if people who have skin cancer and drank more than 1 glass of milk a day are reacting better to this type of drug?”) before deciding to do a clinical trial. If a specialized social network for such community was created, there might be no end to how much data could be gathered. Thing of it as a shotgun approach to medicine.
- 3. Marketing
- Marketing, off course, is all about deep knowledge of the audience. The best way to market a messageÂ is to discover what motivates people and how to craft the message to match the motivations. When combined with the database of intentions, a social network can work as a set of focus groups for messages. Testing different messages on a narrow audience can allow people to better market their products.
- 4. Reputation Management
- The old adage is that “it’s not what you know, it’s who you know” is at the core of social networking. As more and more people are online and more and more interactions are happening between people with weak ties, assessing a person’s reputation is increasingly important. LinkedIn has keyed in on that effort by giving people the ability to “endorse” members of their social network, providing more information about how a person performed in a particular job. In a similar fashion, profiles no Ebay allow buyers and sellers to assess the track record of a buyer or seller before making a transaction. Endorsements by one’s strong ties generally reflects much higher than by someone you don’t know. Thus, social networks can work as the glue to reputation management. It is not enough for people to know that a person is seen as important by some random stranger but when one discovers that their friends or colleagues have endorsed a particular individual, they tend to trust those opinions more heavily.
- Let’s take a pedestrian example: imagine you need to get some electrical work done in your house but don’t know any electricians. By looking at your social network, you could find such an expert with ease as the best electrician might be linked to your friends. In a way, social networks are just an extension of asking people for recommendations. Which brings me to the last opportunity on this list.
- 5. Recommendation

- Recommendation is a very powerful driver to decision making: whether it is for hiring a person, picking a new product, or finding a general direction, humans tend to look to their existing network and do a subconscious "most-like" analysis of the information they receive. For example, Amazon has been very successful with the "people who bought this also bought…" and "people who looked at this also looked at…" features. As they gather more data, patterns emerge.
- Similar approaches can be taken into the search space (where what people linked to or clicked on is ranked higher than other stuff) and in other areas like music (last.fm comes to mind) or other media consumption (for example, the success of aggregator like Digg, techmeme or tailrank can be attributed in large part to the need people have to know what other people think is good).
- Conclusion
- Social Networks should not really be a set of standalone tools but they are essential to building the next set of applications that leverage the power of the crowds. As such, social networking should be a feature and not an end-goal until itself. The companies that understand this basic rule will be the ones that succeed in that space, leveraging opportunities created by social networks in a fashion that will provide unprecedented benefits.

Laws regarding posting inapproiate content on social media (Legal implications of certain online action and content)

1. Voyeurism and violation of privacy
2. Video voyeurism
3. Stalking
4. Sending obscene material without the consent of the recipient
5. Use of child for pornographic purposes
6. Sexual harassment
7. Revenge porn
8. Hacking of account or creating a fake account in someone else's name
9. Video and audio piracy

Most users neither know nor understand the impact or the possible consequences of some of their online activities. Teaching them ethical and moral behaviour in general, and an awareness of children's rights can create empathy for the victims of their communication and may address some problems such as cyberbullying, humiliating comments. However, they also need to be made aware about the legal implications of some of their online actions.

Children may also show extra bravado because they have the illusion that their actions online are anonymous and that "nobody will ever know".

Please note that the following are legal offences: Details of offences and the relevant sections of different legislation have been provided here for the information and knowledge of the

programme planners. These will need to be incorporated according to the evolving capacities of children and young persons and their age appropriate information requirements. These can also be suitably adapted for the different adult stakeholders.

Voyeurism and violation of privacy

Section 354C, the Indian Penal Code (IPC) 1860: Viewing and/or capturing the image of a girl or woman going about her private acts, where she thinks that no one is watching her is a crime. This includes a woman, using a toilet, or who is undressed or in her underwear, or engaged in a sexual act.

It may not be a crime if a girl or woman agrees to taking of her private photos, it can certainly be risky. However, if she expects them to remain with only certain people, then sharing them is a crime. She must expressly consent to both, watching/taking pictures as well as sharing them, for it to not be an offense. The offender in such cases of voyeurism can be punished with three to seven years of imprisonment and a fine. While this section of the IPC can only be used by girls and women, the Information Technology Act, 2000 is gender neutral.

Video voyeurism

Section 66E, IT Act, 2000: Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding Rupees two lakh or with both.

Explanation: For the purposes of this section,

1. “transmit” means to electronically send a visual image with the intent that it be viewed by a person or persons:
2. “capture” with respect to an image, means to videotape, photograph, film or record by any means
3. “private area” means the naked or undergarment clad genitals, pubic area, buttocks or female breast
4. publishes” means reproduction in the printed or electronic form and making it available to public
5. “under circumstances violating privacy” means circumstances in which a person can have a reasonable expectation that
    - he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

- any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

Stalking

Section 354D, IPC, 1860: Continuously following a woman or contacting her, either online or in person, and where she has clearly shown that she does not want the attention is a criminal offence. It is punished by three years for a first offense, and five years for repeat offenses. The only exception is when a person is stalking a woman as a legal duty.

Sending obscene material without the consent of the recipient

Section 354A, IPC, 1860 (sexual harassment): it includes the act of showing pornography against the will of a woman.

Section 67, IT Act, 2000: It punishes sharing obscene material in electronic form. The punishment can be jail for five years and a fine of Rs 10 lakhs.

Section 67A, IT Act, 2000: It punishes sharing material containing sexually explicit act in electronic form with jail for seven years and a fine of Rs 10 lakhs. The provisions of the Information Technology Act are not gender specific and apply to everyone.

Use of child for pornographic purposes

Section 13, Protection of Children from Sexual Offences (POCSO) Act, 2012: Whoever, uses a child in any form of media (including programme or advertisement telecast by television channels or internet or any other electronic form or printed form, whether or not such programme or advertisement is intended for personal use or for distribution), for the purposes of sexual gratification, which includes:

- representation of the sexual organs of a child;
- usage of a child engaged in real or simulated sexual acts (with or without penetration);
- the indecent or obscene representation of a child, shall be guilty of the offence of using a child for pornographic purposes.

Section 14, POCSO Act, 2012:

1. Whoever, uses a child or children for pornographic purposes shall be punished with imprisonment of either description which may extend to five years and shall also be liable to fine and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also be liable to fine.

2. If the person using the child for pornographic purposes commits an offence referred to in section 3, by directly participating in pornographic acts, he shall be punished with imprisonment of either description for a term which shall not be less than ten years but which may extend to imprisonment for life, and shall also be liable to fine.

Section 67, IT Act, 2000 (Publishing or transmitting obscene material in electronic form):
Whoever,

- 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,

shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to Rs 10 lakh.

Section 67A, Information Technology Amendment Act (ITAA), 2008 (Punishment for publishing or transmitting of material containing sexually explicit acts):
Whoever,

- publishes or transmits or causes to be published or transmitted in the electronic form
- any material which contains sexually explicit act or conduct

shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to Rs 10 lakhs and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to Rs 10 lakhs.

Section 67B, IT Act, 2000 (Transmitting material depicting children, including nude or sexually explicit pictures of self, if a child):
Whoever,

- publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or

- creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner or
- cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or
- facilitates abusing children online or
- records in any electronic form own abuse or that of others pertaining to sexually explicit act with children,

shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to Rupees ten lakh and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to Rupees ten lakh:

Sexual harassment

Section 11, POCSO Act, 2012: A person is said to commit sexual harassment to a child when such person with sexual intent;

- utters any word or makes any sound, or makes any gesture or exhibits any object or part of body with the intention that such word or sound shall be heard, or such gesture or object or part of body shall be seen by the child; or
- makes a child exhibit his body or any part of his body so as it is seen by such person or any other person; or shows any object to a child in any form or media for pornographic purposes; or
- shows any object to a child in any form or media for pornographic purposes; or
- any other means; or repeatedly or constantly follows or watches or contacts a child either directly or through electronic, digital or
- threatens to use, in any form of media, a real or fabricated depiction through electronic, film or digital or any other mode, of any part of the body of the child or the involvement of the child in a sexual act; or
- entices a child for pornographic purposes or gives gratification therefor.

Section 12, POCSO Act, 2012: Whoever, commits sexual harassment upon a child shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable for fine.

Section 354A, IPC, 1860: It provides for punishment of jail between one and three years for making a demand for sexual favors and making sexually colored remarks towards a woman

Section 509, IPC, 1860: It deals with word, gesture or act which intends to insult the 'modesty' of a woman.

Section 509 can also be applied for intrusion of privacy intending to insult the modesty of a woman if a person obtains a woman's contact details and tries to contact constantly against her will. The IPC is not very clear about the meaning of "modesty of a woman" but the Courts usually make the determination based on the circumstances surrounding the incident. The Supreme Court referred to 'modesty' as "feminine decency" and a virtue that women possess due to their sex. For Section 509 to apply, the offender should have uttered any word, made a gesture or sound, or exhibited any object, or intruded on the privacy of a woman, with the intention that this should be seen and heard by the woman. The punishment can be a term of simple imprisonment up to three years.

In addition to the above-mentioned provisions in the IPC that that apply only to females, there are other laws which apply generally. Section 294 of the IPC punishes any obscene words uttered in a public place. Section 295A of the IPC punishes words, either written or spoken, which insult someone's religions or religious beliefs. Section 3(1)(x) of the Scheduled Castes and Scheduled Tribes (Prevention of Atrocities) Act deals with caste-based abuse. Section 503 of the IPC deals with threats to injure any person, their reputation, or their property and Section 506 of the IPC provides for a jail term of seven years and a fine as punishment for criminal intimidation.

Revenge porn

Victimizing by way of revenge porn has become a common phenomenon in India now. This is often also practiced by children below 18 years of age. It may be described as "an act whereby a perpetrator satisfies his anger and frustration for a broken relationship through publicizing false, sexually provocative portrayal of his/her victim, by misusing information that he may have known naturally and that he may have stored on his computer, or phone, or may have been conveyed to his electronic device by the victim herself, or may have been stored in the device with the consent of the victim herself; and which may essentially have been done to publicly defame the victim."

While revenge porn essentially creates sexual violence against girls and women, it necessarily involves voyeurism, hacking, stalking, and violation of privacy. There is no specific law for revenge porn but the offences can be regulated by applying Section 354C, IPC (Voyeurism), Section 66E, IT Act (violation of privacy) and Section 509, IPC (harming the modesty of

women). Revenge porn should also be seen in the perspective of indecent representation of women.

Hacking of account or creating a fake account in someone else's name

Section 66C, IT Act, 2000 which deals with identity theft, provides for jail for three years a fine of Rupees one lakh if it is shown that someone stole or dishonestly used another person's password, digital signature, or any other unique identifying feature. Section 66D provides similar punishment for cheating by personation by using a computer source, i.e., if someone creates a fake social media account in someone else's name and cheats anyone through it.

Identity theft, Section 66C IT Act, 2000: Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term that extends up to three years and shall also be liable to fine which may extend to Rupees one lakh.

Section 66D, IT Act (Impersonation), 2000: Whoever, by means of any communication device or computer resource cheats by personation (assumes the identity of someone else with the intention of fooling or deceiving the person) shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to Rupees one lakh.

Section 66B, IT Act, 2000 (Stolen Computer): Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe that the same to be a stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to Rupees one lakh or with both.

Video and audio piracy

Watching movies on copied DVDs or downloaded from Torrent sites may not currently be a crime in India, it certainly is in many countries as such acts constitute infringement of copyright.

In the wake of messages that several internet service providers posted on their websites, the Bombay High Court ruled that "the offense is not in viewing, but in making a prejudicial distribution, a public exhibition or letting for sale or hire without appropriate permission copyright-protected material." The messages by the ISPs, displayed when users try to open blocked websites, said, "Viewing, downloading, exhibiting or duplicating an illicit copy of the contents is punishable as an offence under different sections of the Copyright Act, 1957."

Downloading movies, music and copyright content from the internet is against the Indian copyright law, as are uploading copyright content to the web. By the way, saving images off

the web, uploading them elsewhere like Reddit, making memes out of them, using them in your projects, etc are illegal too. That image does not belong to you; its copyright belongs to someone else, so you can't profit from it without their permission

Best Practices: Safe Social Networking

Safety Tips for Social Networking

Social networking sites like Facebook and Twitter can be a great way to connect with friends. But there are some social networking safety tips you should always keep in mind.

- **Manage your privacy settings.** Learn about and use the privacy and security settings on your social networking sites. They help you control who sees what you post and manage your online experience in a positive way. You'll find some information about Facebook privacy settings at the bottom of this webpage.
- **Remember: once posted, always posted.** Protect your reputation on social networks. What you post online stays online. Think twice before posting pictures you wouldn't want your parents or future employers to see. Recent research found that 70% of job recruiters rejected candidates based on information they found online.
- **Build a positive online reputation.** Recent research also found that recruiters respond to a strong, positive personal brand online. So demonstrate your mastery of the environment and showcase your talents.
- **Keep personal info personal.** Be careful how much personal info you provide on social networking sites. The more information you post, the easier it may be for someone to use that information to steal your identity, access your data, or commit other crimes such as stalking.
- **Protect your computer.** Security start with protecting your computer. Install Antivirus software. Keep your operating system, web browser, and other software current. Visit Microsoft support for information on automatically installing the latest security updates for Office 365 and Windows.
- **Know what action to take.** If someone is harassing or threatening you, remove them from your friends list, block them, and report them to the site administrator.
- **Use strong passwords.** Make sure that your password is at least eight characters long and consists of some combination of letters, numbers, and special characters (for example, +, @, #, or $).
- **Be cautious on social networking sites.** Even links that look they come from friends can sometimes contain harmful software or be part of a phishing attack. If you are at all suspicious, don't click it. Contact your friend to verify the validity of the link first.

Platform Specific Best Practices

Facebook

Managers of Facebook pages at Tufts must be able to check on the page at least once a day and should have enough content to post at least once each week. Each Tufts Facebook page should have at least two staff or faculty members as admins.

- **Do not create a personal profile for a university department, organization or office.** Profiles are designed for individuals only and users may view inappropriate profiles as misleading. Creating a "personal account for anything other than an individual person" is a violation of Facebook's Terms of Service and Facebook warns that violators are at risk of "permanently losing access to the account and all of its content."
- **Avoid posting the same status updates on both Facebook and Twitter.** Some services and applications allow you to post the exact same text and links to both channels at once. Since Twitter and Facebook are different mediums with different audiences, tone, frequency of posts, and strategy and goals, updates to each should be unique. Visually, these statuses often look incorrect since they may go over Twitter's character limit or don't show the link correctly on Facebook. If you want to post the same information on both channels, craft each status so that it makes the most of the style and tools of each platform.
- **Pay attention to your insights.** Facebook insights offer a lot of information on the people who like your page and what they are interested in. Your job is to understand what the insights mean and use them to create posts that will engage your fans, encourage interaction with the page, and attract new likes.
- **Be visually pleasing.** Users visiting your page are drawn to visually appealing layouts and posts. Be sure to highlight photos and other visual posts, remember to delete pasted links in status updates, and edit status so they are not too lengthy.
- **Let your fans speak.** People may sometimes comment on a post or post something on your page's wall that is critical or negative. Correcting a mistake, apologizing and offering better in the future, or providing information about the event in question is often the best way to let the poster know you have heard them. Unless the post is profane, obscene, harassing or threatening, it is not a best practice to delete it. People may also post something very positive on your page – you can allow these posts on your main timeline to bring extra attention to them.

Twitter

Twitter encourages frequent updates, engagement and retweeting content. Account managers at Tufts must be able to login to the account at least once per day and should be able to post often and respond with some immediacy. At least two people in a department should have the password to an official Tufts Twitter account.

- **Listen and Respond**. Don't only monitor those tweets that mention your handle directly, but set up a search so you can keep an ear on what is happening when people do not tag you in their tweet. When it's appropriate, respond or retweet.
- **Avoid posting the same status updates on both Twitter and Facebook**. Some services and applications allow you to post the exact same text and links to both channels at once. Since Twitter and Facebook are different mediums with different

audiences, tone, frequency of posts, strategy and goals, updates to each should be unique. Visually, these statuses often do not look correct since they go over Twitter's character limit or don't show the link correctly on Facebook. If you want to post the same information on both channels, craft each status so that it makes the most of the style and tools of each platform.

- **Use hashtags and mention other users.** Two of the key elements of Twitter is the use of hashtags and the ability to tag other users in your tweets. Hashtags allow users to join a greater conversation, so including one or two relevant hashtags in your tweets will put your tweet in front of more than just your followers. Tagging other accounts in your tweet gives them credit for the material (for example crediting a link to @nytimes) and alerts them that they've been mentioned, which may prompt them to retweet or comment on your tweet.
- **Pay attention to analytics**. Free Twitter metrics are available at analytics.twitter.com. These metrics offer some insight into the reach and popularity of your tweets. Your job is to understand what the metrics mean and use them to create tweets that will engage your fans, encourage retweets and favorites, and attract new followers.
- **Follow the main Tufts University handle and other official Tufts accounts.** We have created multiple lists that include official Tufts Twitter handles, faculty, student groups, campuses, etc. You can follow one or a few of these lists to see what other people and departments are tweeting. It is good practice to follow other Tufts handles and occasionally retweet relevant information.
- **Follow back.** Following back those who follow you is a great relationship builder. Fostering relationships and encouraging interaction is key, so following back relevant, appropriate followers builds goodwill with our audiences.
- **Use a client.** Clients like TweetDeck have many advantages that make them great tools for managing your Twitter account:
    - You can schedule tweets in advance, so even if you cannot check your account continuously, you can schedule appropriate tweets throughout the day.
    - Their interfaces allow you to choose various streams to monitor, so you can monitor tweets that mention you, Tufts' lists, search terms, direct messages, etc.

Instagram

Instagram is a free photo and video sharing app that allows users to apply digital filters, frames and special effects to their photos and videos. Managers of Instagram accounts at Tufts should check on the account at least once each day and have enough content to post a few times each week.

- **Use hashtags**. Like Twitter, Instagram uses tags. Tagging your photos means that more people may see them, since they may be searching that tag. But be careful: too many tags can be seen as spammy.
- **Interact with others.** Search for photos that may be relevant to your department, office or group. Interact with others by liking and commenting on photos that are relevant to you.
- **Tag locations**. Tagging the location where the photo was taken gives some context to the image.
- **Consider stories.** Instagram stories are special photos and videos that are seen by followers for just 24 hours. They appear at the top of the Instagram feed.

Blogs/Tumblr

Managers of blogs at Tufts should be able to check on the blog at least once a day and should have enough content to post consistently.

- **Make your blog a conversation.** Your blog is not the only thoughts on the subject, so raise questions, introduce other ideas and allow people to comment and continue the conversation. Monitor the comments you receive in order to weed out spam and delete any inappropriate submissions.
- **Encourage readers to share your posts.** Increase traffic to your blog by making it easy for readers to share the content on social media. Most platforms allow sharing plugins so make sure each blog post can be shared on at least Facebook and Twitter. Many blogs also include options for sharing on Tumblr, Pinterest, Google+, Digg and Reddit.
- **Make friends in the blogosphere.** Do a little research and find other blogs that cover similar topics or are authored by similar bloggers. You can subscribe to these blogs so you know when they are posting. Comment and link to their post if they say something you want to reference. You can add these related blogs as well as Tufts blogs to your blogroll, which often appears in the sidebar.
- **Own your opinion:** Blogs often feature the author's opinion and it's ok to share yours. Keep in mind that you are a representative of Tufts, but that the opinions expressed in the blog are yours. If you are expressing a strong opinion, remind your readers that it is your view, not that of the university.

Flickr

Flickr is an image and video hosting website and online community. Photos can be shared on Facebook and Twitter and other social networking sites.

- **Share only original photos**. Due to copyright issues, you should only post your own original photos to Flickr. You can indicate photos that are copyright protected by including "© Tufts University." See the Tufts Social Media Policy For Official Social Media Accounts for more information on copyright rules.
- **Tag your photos**. Tagging your photos makes it easier for users to find your images in searches. Be sure to include "Tufts" or "Tufts University" tags.
- **Provide a title and description for every image posted**. It's important to give context to your photos. Image titles and descriptions are also used as search criteria and making sure to include them will help others find your photos.

YouTube/Vimeo

YouTube and Vimeo are video hosting/sharing platforms that showcase a variety of user-generated content. Videos can be shared on other social sites or taken from the platforms and embedded directly on a user's blog or website.

- **Don't use copyrighted material.** If your video is set to music, you must use royalty-free music and sound effects. To use a copyrighted piece, you must contact the owner. Most often the owner or publisher will be listed on sheet music or a CD label. See the Tufts Social Media Policy For Official Social Media Accounts for more information on copyright rules.

- **Use proper credits.** If you are creating video content for the university, include a credits slide at the end of all videos with, at minimum, a message that says (c) [year] Tufts University.
- **Include "Tufts" in your file names.** Including the word "Tufts" in the naming of your raw video file will help enhance your SEO. (e.g. from "StudyAbroadProfile.mov" to "TuftsStudyAbroadProfile.mov").
- **Make your content accessible.** Captioning technology has progressed to the point to where it is affordable and straightforward to implement. Read more about how to create captions and subtitles on YouTube.

LinkedIn Groups

Managers of LinkedIn groups at Tufts should be able to check on the group every few days and should have content to provide to the members.

- **Don't focus on "selling" your organization/entity.** Rather, put the focus on the group and members. Provide content that is appealing to them.
- **Carry on the conversation**. Facilitate group discussions by posting useful information and prompts for future discussions.
- **Make introductions between members.** Simple introductions can add a personal touch to your group members' experience.
- **Promote the group.** Promote your group to your personal LinkedIn network or by posting the group URL on external websites and marketing materials.

How to write a social media case study (with template)

What is a social media case study?

A case study is basically a long testimonial or review. Case studies commonly highlight what a business has achieved by using a social media service or strategy, and they illustrate how your company's offerings help clients in a specific situation. Some case studies are written just to examine how a problem was solved or performance was improved from a general perspective. For this guide, we'll be examining case studies that are focused on highlighting a company's own products and services.

Case studies come in all content formats: long-form article, downloadable PDF, video and infographic. A single case study can be recycled into different formats as long as the information is still relevant.

At their core, case studies serve to inform a current or potential customer about a real-life scenario where your service or product was applied. There's often a set date range for the campaign and accompanying, real-life statistics. The idea is to help the reader get a clearer understanding of how to use your product and why it could help.

Broad selling points like "our service will cut down your response time" are nice but a sentence like "After three months of using the software for responses, the company decreased their response time by 52%" works even better. It's no longer a dream that you'll help them decrease the response time because you already *have* with another company.

So now that you understand what a case study is, let's get started on how to create one that's effective and will help attract new clients. How to write a social marketing case study

Writing an effective case study is all about the prep work. You've got to get all of the questions and set up ready so you can minimize lots of back and forth between you and the client.

1. Prepare your questions

Depending on how the case study will be presented and how familiar you are with the client to be featured, you may want to send some preliminary questions before the interview. It's important to not only get permission from the company to use their logo, quotes and graphs but also to make sure they know they'll be going into a public case study.

Your preliminary questions should cover background information about the company and ask about campaigns they are interested in discussing. Be sure to also identify which of your products and services they used. You can go into the details in the interview.

Once you receive the preliminary answers back, it's time to prepare your questions for the interview. This is where you'll get more information about how they used your products and how they contributed to the campaign's success.

2. Interview

When you conduct your interview, think ahead on how you want it to be done. Whether it's a phone call, video meeting or in-person meeting, you want to make sure it's recorded. You can use tools like Google Meet, Zoom or UberConference to host and record calls (with your client's permission, of course). This ensures that your quotes are accurate and you can play it back in case you miss any information. Tip: test out your recording device and process before the interview. You don't want to go through the interview only to find out the recording didn't save.

Ask open-ended questions to invite good quotes. You may need to use follow-up questions if the answers are too vague. Here are some examples.

- Explain how you use (your product or service) in general and for the campaign. Please name specific features.
- Describe how the feature helped your campaign achieve success.
- What were the campaign outcomes?
- What did you learn from the campaign?

Since we're focused on creating a social media case study in this case, you can dive more deeply into social strategies and tactics too:

- Tell me about your approach to social media. How has it changed over time, if at all? What role does it play for the organization? How do you use it? What are you hoping to achieve?
- Are there specific social channels you prioritize? If so, why?
- How do you make sure your social efforts are reaching the right audience?
- What specific challenges do organizations like yours face when it comes to social?

- How do you measure the **ROI of using social**? Are there certain outcomes that prove the value of social for your organization? What metrics are you using to determine how effective social is for you?

As the conversation continues, you can ask more leading questions if you need to to make sure you get quotes that tie these strategic insights directly back to the services, products or strategies your company has delivered to the client to help them achieve success. Here are just a couple of examples.

- Are there specific features that stick out to you as particularly helpful or especially beneficial for you and your objectives?
- How are you using (product/service) to support your social strategy? What's a typical day like for your team using it?

At the end of the interview, be sure to thank the company and request relevant assets.

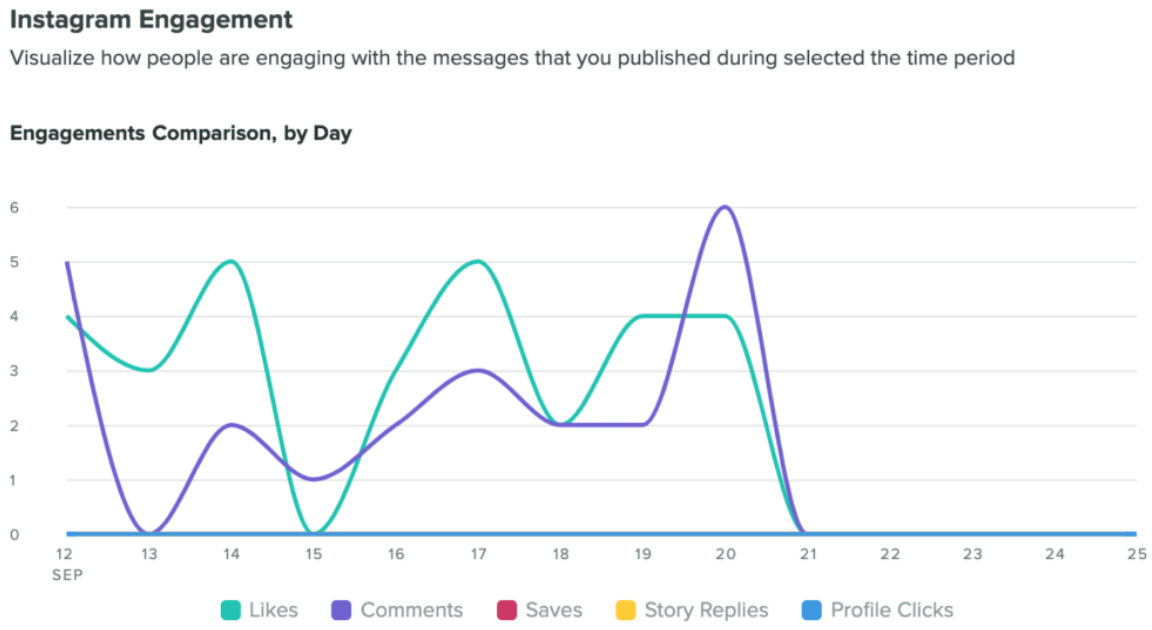
Afterwards, you may want to transcribe the interview to increase the ease of reviewing the material and writing the case study. You can DIY or use a paid service like Rev to speed up this part of the process.

3. Request assets and graphics

This is another important prep step because you want to make sure you get everything you need out of one request and avoid back and forth that takes up both you and your customer's time. Be very clear on what you need and the file formats you need them in.

Some common assets include:

- Logo in .png format
- Logo guidelines so you know how to use them correctly
- Links to social media posts that were used during the campaign
- Headshots of people you interviewed
- Social media analytics reports. Make sure you name them and provide the requested date range, so that if you're using a tool like Sprout, clients know which one to export.



For graphics, Sprout's reports make it easy to pull presentation-ready graphs to insert into the case study. All the client needs to do is export the relevant report and send it over to you to crop.

In the **Keele University case study by Sprout**, we examined how the university built their brand with Sprout. It includes examples of social media posts and the above graph to examine their year-over-year audience growth of 10.1% across their group.

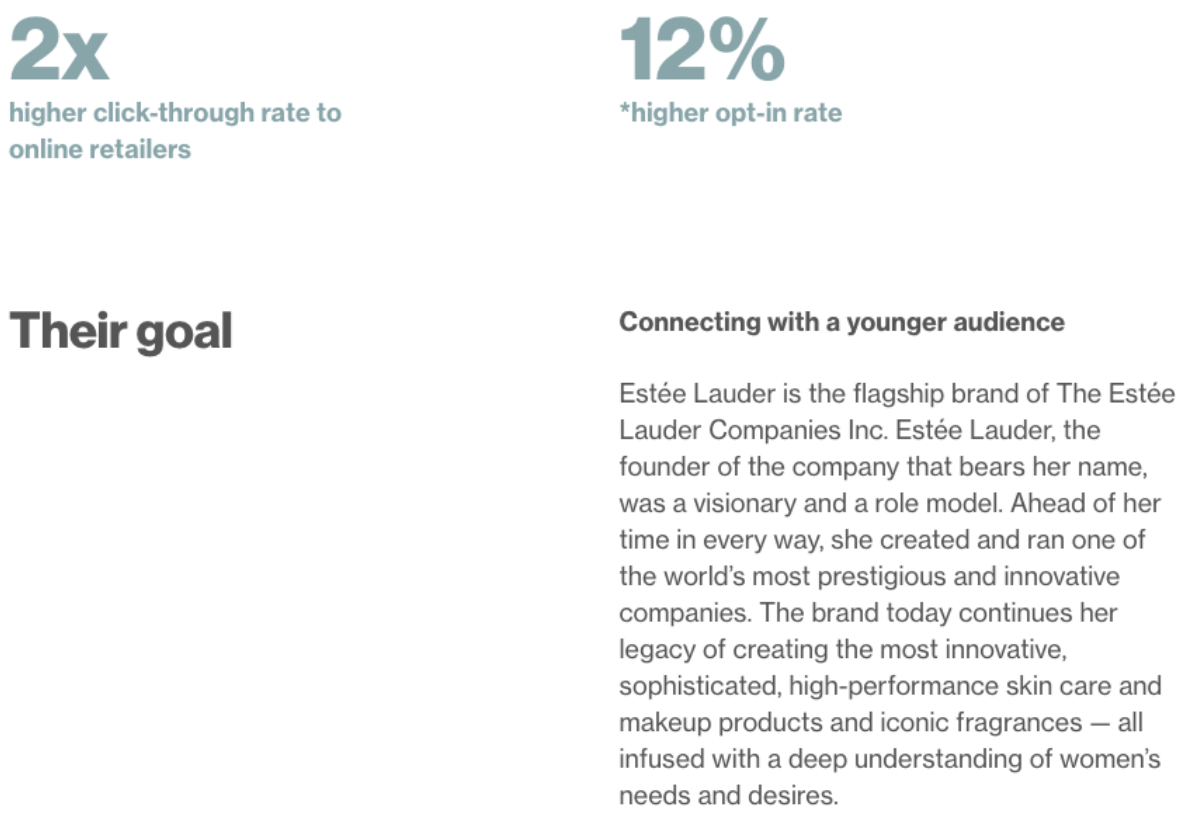
4. Write the copy

Now that the information has been collected, it's time to dissect it all and assemble it. At the end of this guide, we have an example outline template for you to follow. When writing a case

study, you want to write to the **audience that you're trying to attract**. In this case, it'll be a potential customer that's similar to the one you're highlighting.

Use a mix of sentences and bullet points to attract different kinds of readers. The tone should be uplifting because you're highlighting a success story. When identifying quotes to use, remove any fillers ("um") and cut out unnecessary info.

Your copy should read somewhat like an adventure story: introduce the character, conflict emerges, a solution appears and the hero conquers the problem. Keep this story arc in mind while you're assembling your copy.



Pinterest's business advertising **case study of Estee Lauder** clearly breaks down each section in a presentable way. Their headers are to the point so you can scroll to them. The body for each section includes short paragraphs and digestible sentences.

5. Pay attention to formatting

Case studies can be long so you want to make sure you keep your reader's attention throughout the piece. In terms of copy, this means that you should give thought to your headline and subheaders. Then, identify quotes that can be pulled and inserted into the piece. Next, insert the relevant social media examples and metric graphs. You want to break up the paragraphs of words with images or graphics. These can be repurposed later when you share the case study on social media, email or sales decks.

CASE STUDIES

How Stoneacre Motor Group achieved £1 million in sales using Sprout Social

73.5%
YoY increase in total social followers

100%
YoY increase in total social engagements

153.2%
YoY increase in total social impressions

In the **Sprout case study of Stoneacre Motor Group**, we added three statistics right below the header. They're succinct and grabs the reader's attention.

And finally, depending on the content type, enlist the help of a graphic designer to make it look presentable. You may also want to include call-to-action buttons or links inside of your article. If you offer free trials, case studies are a great place to promote them.

Social media case study template

Writing a case study is a lot like writing a story or presenting a research paper (but less dry). This is a general outline to follow but you are welcome to enhance to fit your needs.

Headline

- Attention-grabbing and effective.
- Example: "**How Benefit turns cosmetics into connection using Sprout Social**"

Summary

- A few sentences long with a basic overview of the brand's story.
- Give the who, what, where, why and how.
- Which service and/or product did they use?

Introduce the company

- Give background on who you're highlighting.
- Include pertinent information like how big their social media team is, information about who you interviewed and how they run their social media.

Describe the problem or campaign

- What were they trying to solve?
- Why was this a problem for them?
- What were the goals of the campaign?

Present the solution and end results

- Describe what was done to achieve success.
- Include relevant social media statistics (graphics are encouraged).

Conclusion

- Wrap it up with a reflection from the company spokesperson.
- How did they think the campaign went? What would they change to build on this success for the future?
- How did using the service compare to other services used in a similar situation?

Conclusion

Case studies are essential marketing and sales tools for any business that offer robust services or products. They help the customer reading them to picture their own company using the product in a similar fashion. Like a testimonial, words from the case study's company carry more weight than sales points from the company.

When creating your first case study, keep in mind that preparation is the key to success. You want to find a company that is more than happy to sing your praises and share details about their social media campaign.

Once you've started developing case studies, find out the best ways to promote them alongside all your other content with our **free social media content mix tool**.

UNIT–IV: Introduction to Intellectual Property Rights (IPR)

Introduction to IPR

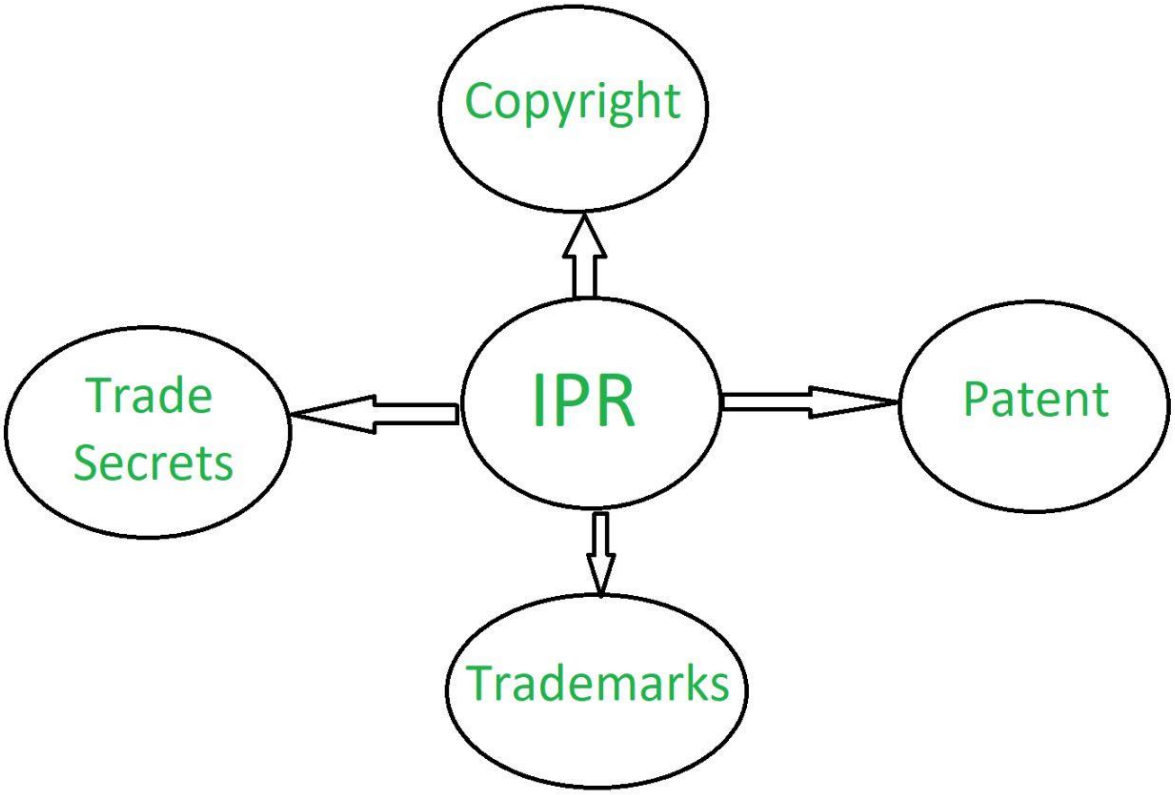
Intellectual property rights are the rights given to every person for creating new things according to their minds. IPR usually gives the creator a complete right over the use of his/her creation for a certain period of time.

Intellectual property rights are the legal rights that cover the benefits given to individuals who are the owners and inventors of work and have created something unique with their intellectual creativity or capability. Every person related to areas such as literature, music, invention, etc., can be granted such rights, which can then be used in their business practices by them.

The creator/inventor gets complete rights against any misuse or use of work without his/her prior information. However, the rights are issued for a limited period of time to maintain equilibrium.

1. Industrial designs
2. Scientific discoveries
3. Protection against unfair competition
4. Literary, artistic, and scientific works
5. Inventions in all fields of human endeavor
6. Trademarks, service marks, commercial names, and designations

Types of Intellectual Property Rights:
Intellectual Property Rights can be classified into four types:



1. **Copyright:** Copyright is a term that describes ownership or control of the rights to the use and distribution of certain works of creative expression, including books, videos, movies, music, and computer programs.
2. **Patent:** A patent gives its owner the right to exclude others from making, using, selling, and importing an invention for a limited period of time. The patent rights are granted in exchange for enabling public disclosure of the invention.
3. **Trademark:** A Trademark is a Graphical representation that is used to distinguish the goods and services of one party from those of others. A Trademark may consist of a letter, number, word, phrase, logo, graphic, shape, smell, sound, or combination of these things.
4. **Trade Secrets:** Trade secret describes the general formula of any product and the key behind any organization's progress. It also includes various firms' different secret formulas for the same products which differ in quality.

Advantages of Intellectual Property Rights:

The advantages of intellectual property rights are as follows:

- IPR yields exclusive rights to the creators or inventors.
- It encourages individuals to distribute and share information and data instead of keeping it confidential.
- It provides legal defense and incentivizes the creators for their work.
- It helps in social and financial development.
- It inspires people to create new things without fear of intellectual theft.

International Instruments Relating to the Protection of Intellectual Property

"In today's economic environment, intangible assets are becoming increasingly important. These assets, which are the result of human intellectual creative activity such as invention, design, know-how, and artistic creation, are known as "intellectual property." Some forms of Intellectual property rights are specifically entitled to legal protection such as trademarks, designs, literary works, layout designs and trade secrets. In the recent years we have seen an increase in the volume of trade of good and services relating to intellectual property.

Therefore the protection of intellectual property necessary otherwise it will lead to distort free trade. The protection regarding intellectual property has been always a narrow in most of the developing countries. Some developed countries also have problematic intellectual property regimes that, for example, openly discriminate against foreign nations, provide excessive protection, or otherwise have regimes so different from those employed by the rest of the world that its administration is discriminatory. This trade distorts were needed to be addressed and for the purpose of same the WTO decided to establish framework for the protection of intellectual property. There were number of treaties formed as a common legal framework for the protection of intellectual property right. In this article the following three of the major frameworks are discussed-

1. Berne Convention for the protection for Artistic and Literary works.
2. The Paris Convention for the Protection of Industrial Property
3. TRIPS (Agreement on the trade related aspects of intellectual property rights)

Contents

3. TRIPS (Agreement on the trade related aspects of Intellectual Property Rights)

Berne convention for the protection for Artistic and Literary Works-
Global defense of copyright started on the basis of bilateral treaties at approximately mid-19th century. A number of these treaties were signed which provided for the mutual recognition of rights but they were neither adequately detailed nor uniform. The need for a standardized structure led to the Berne Convention on the Protection of Literary and Artistic works being established and adopted on 9th September 1886. The Berne convention is the oldest copyright international treaty. This treaty is open and available to all the nations in the world. The ratification process or power of this treaty lies with the World Intellectual Property Organization Director General. The preamble of Berne Convention describes the purpose of this treaty. It says that "to *protect. in as effective and uniform a manner as possible, the rights of authors in their literary and artistic works"*

The convention's three fundamental principles are –

1. The convention convers the concept of protection independence which means that the rights granted are indented form the protection that exists in the country of origin for the work and their use.
2. The national care provided will not be formal, i.e. automatic security is granted and there is registration formality, deposit formality, etc.
3. The principle of 'national treatment' of the convention's basis is that one of the member states must be protected by the same level of protection as these grants to works of its nationals in each of the member states.

This convention provides protection to works like any original literary, scientific and artistic production whatever, its mode of expression, is unlimited, as it is mentioned in Article 2 of the conceptions. Works based or derived or translated from already existing works like music or other literary works or artistic modification are also protected under this convention. The convention provides with the concept of folklore which means that every member states has an option to protect any unpublished work where the identity of the author is unknown but the author will be presumed by designation of nation legacy of the author to be a national of that country. This convention provides protection to the authors of works, whether they are published or unpublished, when that are the resident of the member state in accordance to the article 3 of the convention and in case they are not the residents or national so if the member stated, for the first time they need to publish their work in a member state. The section 2(6) of the conventions mentions that the convention's defense shall operate on behalf of the author and his successors.

Some of the articles related to rights are-

Article 8- "The exclusive rights granted to authors under the Convention include the right to translate"

Article 9- "the right to reproduce in any manner or form, including any sound or visual recording"

Article 11-"the right to perform dramatic, dramatic, musical and musical works"

obligations or rules requiring the Member States to legislate or permit them to enact legislation pursuant to those rules; the fourth category encompasses the institutional structure for the application of the Convention and includes the Convention's final clauses." The right of priority provides that if the same applicant of his successor his applying he may seek protection in all other member states within a specified period of time.

""*National treatment" means that each country party to the Paris Convention must give nationals from the other Member States the same level of protection as it provides to its own nationals with regard to the protection of industrial property. Articles 2 and 3 of the Convention provide for the relevant provisions. The law on national treatment not only ensures the rights of foreigners but also the absence of any discrimination towards them."*

- **Independence Of Patents-**

Inventions granted to nationals or residents of the member states in the member states shall be treated as indented from invention patents obtained in other countire4s, including non-member countries, in respect of the same invention. The rule regarding the indented of the invention patents is mentioned in Article 4 of the convention. The grant of a patent for invention for a given invention does not impose a compulsory patent for the same invention on any other Member State. His rule would, for example, be violated by a provision in the national legislation which starts with the invention patent from (foreign) the priority date and not with the filing date of the application in the country. The inventor must have the right to be mentioned in the patent for invention as such, according to a general rule. Article 4 stipulates this.

"*Article 4bis(5) contains a special feature of the principle of patent independence for invention. The provisions require that, if no priorities had been claimed, a patent granted in respect of an application claiming the priority of one or more foreign applications should be given the same duration as would have been granted under national law. In other words, the priority period shall not be deducted from the duration of a patent invoking the first application's priority."*

- **Use of Trademarks**

Article 5C regulates the criteria for the use of registered trademarks (1). Some countries which provide for the registration of a trademark also require that trademarks be used after registration within a certain time period. If this use is not complied with, the label may be expunged from the register

Usage usually implies the selling of marked items even though the use of the label may be limited more widely by national laws. "Use" means the selling of goods labelled. The Convention protects 'well-known trademarks' in Article 6bis. This Article obliges a Member State to deny or cancel registration by prohibiting the use in that Member State of a mark which may cause confusion with another mark which is already well-known..The provisions of this Article the aim of the article is to extend protection to a trademark which, although not registered in or used in a Member State, is well known in that Member State. Isle 5 of the Paris Convention covers industrial designs. This provision simply stipulates the obligation to protect industrial designs by all Member States.

There is no mention of how to provide the defense. Consequently, the Member States can comply with this duty by enacting special legislation on the safety of industrial designs. However, they can also fulfill this duty by granting such rights in compliance with copyright

or unfair competition legislation. Entry to the Paris Convention shall be made by depositing an instrument of accession with the Director-General of the WIPO, as provided for in Article 21. The Convention enters into force three months after accession with respect to a nation that has such a country.

Thus, it adhered to the Convention and was informed by the Director-General of WIPO to all the governments of the Member States. Consequently, accession only requires unilateral action by the country concerned and requires no decision by the competent authorities of the Union.

TRIPS (Agreement on the trade related aspects of Intellectual Property Rights)
The Uruguay Round of multilateral trade negotiations under the General Tariff and Trade Agreement('GATT ') came to an end on 15 December 1993. The Agreement creating the World Trade Organization (the "WTO Agreement") was signed on 15 April 1994. These talks involved, for the first time, debates on international trade-related aspects of intellectual property rights within the GATT. The agreement was the result of these talks. The WTO agreement, including the TRIPS agreement, was concluded on 1 January 1995 (which shall be binding on all WTO members). In the earlier agreement, a new organisation, the World Trade Organization, was formed and starts its activities on 1st januray 1995.

As regards the essence and extent of the TRIPS obligations, the basic principle is that the members should apply the provisions of the Agreement and give the care provided for in the Agreement to the nationals of other members. A 'national' means natural or legal persons liable for immunity where all the members of the World Trade Organization are also bound by the conventions of Paris, Berne and Rome and, with regard to the Integrated Circuits, by the Washington Treaty on Intellectual Property.

Article 14- "the right to broadcast and communicate to the public via wire, re-transmission, loudspeaker or any other means of communication, the right to make film adaptations and to reproduce a work."

The Berne convention also provides with provisions which provides limitations on the application of the rules on specific exclusive rights. The purpose of these provisions is to provide a kind of counterbalance to the minimum standards of security.

The Paris Convention for the protection of industrial property
There was no recognition of protection for industrial property rights existed due to the diversity of laws. It was also difficult to protection for industrial property rights in various countries. In almost all countries the patent application had to be made nearly concurrently to prevent a publication in one count4ry losing the invention's novelty in their country. With the passage of time it became important to provide protection IPR laws in both patent and the trademark. The way to di this was by creating a more internationally oriented technical stream and growing international trade. In 1883 a Diplomatic Conference was held in Par5is and the Paris convention for the protection or defense of industrial property was given the final approval and signature. The Paris convention only had 11 states signatures initially but it increased its membership very significantly during the first quarter of the 20th century.

"The provisions of the Paris Convention can be subdivided into four main categories: firstly, the rules of substantive law which guarantee in each Member State a fundamental right known as the right to national treatment, secondly, a basic right is known as a right is known as a right

of priority; a 3rd category shall describe a number of common rules in the field of substantive law which shall include either rules establishing natural and legal persons' rights and

National Treatment- In accordance with the provisions of the Paris, the Berne, the Rome Convention and the IPIC Treaty, the TRIPS lays down the principle of national treatment which requires a Member to grant treatment to nationals of other Members specified by the Memorandum of Understanding (Memorandum of Understanding). This principle applies to all rights as regards industrial property and copyright. As far as rights are concerned, the obligations only apply in respect of those rights provided under the Convention in the case of actors, phonogram producers and broadcasting organizations.

MFN- The TRIPS Agreement covers the most-favoured-nation concept, which has not historically been formulated in the sense of multilateral intellectual property rights. This principle specifies that the nationality of all other Members shall be consistent with the nationality of the other Members. As is the case with national processing, the procedure for acquisitions or maintenance of intellectual property rights provided for in multilateral agreements concluded under the auspices of the WIPO is excluded from this principle.

Protection of Existing Subject Matter- The TRIPS Agreement includes unique clauses relating to the effect of the Intellectual Property Rights Agreement on the Member on the date of implementation of the Agreement. While the Agreement does not give rise for the Member in question to obligations with respect to acts occurring before the date of application of the Agreement (Article 70.1), the Agreement gives rise, in relation to all subject matter to obligations existing and protected on the day the Agreement is applied or which then or then meet the criteria for protection.

Part II of the TRIPS Agreement sets out minimum standards for the availability, scope, and use of rights of intellectual property. It covers eight parts relating to copyright, trademarks, geographical indications, industrial designs, patents, designs for integrated circuits, defense of undisclosed knowledge, and enforcement of anti-competitive practices in the field of contract licensing.

- Section 1- Copyright and related rights;
- Section 2- Trademark
- Section 3- Geographical indications
- Section 4 Industrial Designs
- Section 5- Patents
- Section 6- Topographies or Layouts of Integrated Circuits

The TRIPS Agreement includes procedures for the protection of intellectual property rights to permit effective action to be taken against any infringement of the intellectual property rights protected by the Agreement, including swift remedies for the prevention of infringements. The procedures should be applied in such a way as to prevent and safeguard valid trade barriers against their violation. Regulation processes should be reasonable and fair, not overly difficult or costly, nor unjustified deadlines or delays.

Conclusion-

The aim of these agreements was not only to provide for, but also to provide for, a minimum standard for the security of the IPR. These agreements establish a basic requirement for IPR compliance that allows right holders to, by civil court or administrative proceedings, defend their legitimate interests. The responsibilities of Member States to create administrative and

judicial processes by which IPR holders may seek effective protection of their interests are laid down in Part III of the Agreement on Implementation of IPR. The general obligation of the Member States to provide compliance mechanisms requires that, under their national law, the enforcement process be available to enable effective action to be taken against any act of infringement of the IPR protected by those agreements, including the inclusion of immediate measures to avoid infringements and remedies. Member countries are expected to ensure that compliance procedures are "fair and equitable" and "not unnecessarily complex or expensive, or to avoid unreasonable deadlines or unreasonable delays."

WTO-WIPO cooperation agreement (WIPO – TRIPS – WTO)

Agreement Between the World Intellectual Property Organization and the World Trade Organization

Preamble

The World Intellectual Property Organization (WIPO) and the World Trade Organization (WTO),

Desiring to establish a mutually supportive relationship between them, and with a view to establishing appropriate arrangements for cooperation between them,

Agree as follows:

Article 1
Abbreviated Expressions

For the purposes of this Agreement:

(i) "WIPO" means the World Intellectual Property Organization;

(ii) "WTO" means the World Trade Organization;

(iii) "International Bureau" means the International Bureau of WIPO;

(iv) "WTO Member" means a party to the Agreement Establishing the World Trade Organization;

(v) "the TRIPS Agreement" means the Agreement on Trade-Related Aspects of Intellectual Property Rights, Annex 1C to the Agreement Establishing the World Trade Organization;

(vi) "Paris Convention" means the Paris Convention for the Protection of Industrial Property of March 20, 1883, as revised;

(vii) "Paris Convention (1967)" means the Paris Convention for the Protection of Industrial Property of March 20, 1883, as revised at Stockholm on July 14, 1967;

(viii) "emblem" means, in the case of a WTO Member, any armorial bearing, flag and other State emblem of that WTO Member, or any official sign or hallmark indicating control and warranty adopted by it, and, in the case of an international intergovernmental organization, any armorial bearing, flag, other emblem, abbreviation or name of that organization.

Article 2
Laws and Regulations

(1) [Accessibility of Laws and Regulations in the WIPO Collection by WTO Members and Their Nationals] The International Bureau shall, on request, furnish to WTO Members and to nationals of WTO Members copies of laws and regulations, and copies of translations thereof, that exist in its collection, on the same terms as apply to the Member States of WIPO and to nationals of the Member States of WIPO, respectively.

(2) [Accessibility of the Computerized Database] WTO Members and nationals of WTO Members shall have access, on the same terms as apply to the Member States of WIPO and to nationals of the Member States of WIPO, respectively, to any computerized database of the International Bureau containing laws and regulations. The WTO Secretariat shall have access, free of any charge by WIPO, to any such database.

(3) [Accessibility of Laws and Regulations in the WIPO Collection by the WTO Secretariat and the Council for TRIPS]

(a) Where, on the date of its initial notification of a law or regulation under Article 63.2 of the TRIPS Agreement, a WTO Member has already communicated that law or regulation, or a translation thereof, to the International Bureau and that WTO Member has sent to the WTO Secretariat a statement to that effect, and that law, regulation or translation actually exists in the collection of the International Bureau, the International Bureau shall, on request of the WTO Secretariat, give, free of charge, a copy of the said law, regulation or translation to the WTO Secretariat.

(b) Furthermore, if, for the purposes of carrying out its obligations under Article 68 of the TRIPS Agreement, such as monitoring the operation of the TRIPS Agreement or providing assistance in the context of dispute settlement procedures, the Council for TRIPS of the WTO requires a copy of a law or regulation, or a copy of a translation thereof, which had not previously been given to the WTO Secretariat under subparagraph (a), and which exists in the collection of the International Bureau, the International Bureau shall, upon request of either the Council for TRIPS or the WTO Secretariat, give to the WTO Secretariat, free of charge, the requested copy.

(c) The International Bureau shall, on request, furnish to the WTO Secretariat on the same terms as apply to Member States of WIPO any additional copies of the laws, regulations and translations given under subparagraph (a) or (b), as well as copies of any other laws and regulations, and copies of translations thereof, which exist in the collection of the International Bureau.

(d) The International Bureau shall not put any restriction on the use that the WTO Secretariat may make of the copies of laws, regulations and translations transmitted under subparagraph (a), (b) or (c).

(4) [Laws and Regulations Received by the WTO Secretariat from WTO Members]

(a) The WTO Secretariat shall transmit to the International Bureau, free of charge, a copy of the laws and regulations received by the WTO Secretariat from WTO Members under Article 63.2 of the TRIPS Agreement in the language or languages and in the form or forms in which they were received, and the International Bureau shall place such copies in its collection.

(b) The WTO Secretariat shall not put any restriction on the further use that the International Bureau may make of the copies of the laws and regulations transmitted under subparagraph (a).

(5) [Translation of Laws and Regulations] The International Bureau shall make available to developing country WTO Members which are not Member States of WIPO the same assistance

for translation of laws and regulations for the purposes of Article 63.2 of the TRIPS Agreement as it makes available to Members of WIPO which are developing countries.

Article 3
Implementation of Article 6ter of the Paris Convention for the Purposes of the TRIPS Agreement

(1) [General]

(a) The procedures relating to communication of emblems and transmittal of objections under the TRIPS Agreement shall be administered by the International Bureau in accordance with the procedures applicable under Article 6ter of the Paris Convention (1967).

(b) The International Bureau shall not recommunicate to a State party to the Paris Convention which is a WTO Member an emblem which had already been communicated to it by the International Bureau under Article 6ter of the Paris Convention prior to January 1, 1996, or, where that State became a WTO Member after January 1, 1996, prior to the date on which it became a WTO Member, and the International Bureau shall not transmit any objection received from the said WTO Member concerning the said emblem if the objection is received by the International Bureau more than 12 months after receipt of the communication of the said emblem under Article 6ter of the Paris Convention by the said State.

(2) [Objections] Notwithstanding paragraph (1)(a), any objection received by the International Bureau from a WTO Member which concerns an emblem that had been communicated to the International Bureau by another WTO Member where at least one of the said WTO Members is not party to the Paris Convention, and any objection which concerns an emblem of an international intergovernmental organization and which is received by the International Bureau from a WTO Member not party to the Paris Convention or not bound under the Paris Convention to protect emblems of international intergovernmental organizations, shall be transmitted by the International Bureau to the WTO Member or international intergovernmental organization concerned regardless of the date on which the objection had been received by the International Bureau. The provisions of the preceding sentence shall not affect the time limit of 12 months for the lodging of an objection.

(3) [Information to Be Provided to the WTO Secretariat] The International Bureau shall provide to the WTO Secretariat information relating to any emblem communicated by a WTO Member to the International Bureau or communicated by the International Bureau to a WTO Member.

Article 4
Legal-Technical Assistance and Technical Cooperation

(1) [Availability of Legal-Technical Assistance and Technical Cooperation] The International Bureau shall make available to developing country WTO Members which are not Member States of WIPO the same legal-technical assistance relating to the TRIPS Agreement as it makes available to Member States of WIPO which are developing countries. The WTO Secretariat shall make available to Member States of WIPO which are developing countries and are not WTO Members the same technical cooperation relating to the TRIPS Agreement as it makes available to developing country WTO Members.

(2) [Cooperation Between the International Bureau and the WTO Secretariat] The International Bureau and the WTO Secretariat shall enhance cooperation in their legal-technical assistance and technical cooperation activities relating to the TRIPS Agreement for developing countries, so as to maximize the usefulness of those activities and ensure their mutually supportive nature.

(3) [Exchange of Information] For the purposes of paragraphs (1) and (2), the International Bureau and the WTO Secretariat shall keep in regular contact and exchange non-confidential information.

Article 5
Final Clauses

(1) [Entry into Force of this Agreement] This Agreement shall enter into force on January 1, 1996.

(2) [Amendment of this Agreement] This Agreement may be amended by common agreement of the parties to this Agreement.

(3) [Termination of this Agreement] If one of the parties to this Agreement gives the other party written notice to terminate this Agreement, this Agreement shall terminate one year after receipt of the notice by the other party, unless a longer period is specified in the notice or unless both parties agree on a longer or a shorter period.

Laws related to IPR

Intellectual property, in basic terms, refers to specific types of intangible assets which have been created (owing to application of one's mental faculties). The requirements for obtaining registration for intellectual properties may vary as per the type of asset under consideration. The ownership of intellectual property rights affords various rights for protection and commercialization of such assets (which are protected by the law of intellectual property).

Intellectual property rights are classified in a universal manner across the globe (with minor jurisdiction-specific changes in terminology as well as requirements for registration). In India specifically, the different forms of intellectual property rights are – Copyright; Trademarks; Patents; Geographical Indications; Designs; Semiconductor integrated circuit layouts and Plant varieties. Each of the aforementioned types of intellectual property rights have been discussed in detail below:

What are the different types of Intellectual Property Rights in India

1. The Copyrights Act, 1957 ("Copyright Act")

Copyright protects the expression of an idea rather than the idea itself. Under section 13 of the Copyright Act, a protection under copyright can be obtained for 'original literary, dramatic, musical and artistic works; cinematograph films; and sound recording'. Interestingly, a copyright protection can also be obtained for computer programmes. A copyright is an 'exclusive right' that is granted to a person to do or authorize to carry out certain activities with regards the copyrighted work. For eg: in case of a literary, dramatic or musical work, the owner (or any person authorized by the owner) is permitted to perform the work; make translation(s) of such work; make adaptations of the work, etc.

The Copyright Act, under section 17, clearly states that the author of the original work (for which protection under copyright has been obtained) shall be the first owner of the work. Further, the owner has the right to license the copyright of their work to third-parties through a written agreement.

In case of published literary works, dramatical works and artistic works, copyright protection shall be provided to such works for a term of 60 (sixty) years in addition to the life of the author.

Incidental to the protection awarded under a copyright, the Copyright Act, also confers certain special rights on the author, under section 57. An author/ owner of the copyright work, even after assigning the work to another person (wholly or partially), has the right to 'claim authorship of the work' and the right to 'claim damages' with respect to any 'distortion, mutilation or modification' of the author's original work, in the event such distortion or any other act is damaging to the author's reputation.

2. The Trade Marks Act, 1999 ("Trade marks Act")

The Trade Marks Act, under section 2(zb) defines a 'trade mark' as 'a mark capable of being represented graphically and which is capable of distinguishing the goods or services of one person from those of others and may include shape of goods, their packaging and combination of colours…'. In simpler words, a trademark provides protection for symbols, colours, shapes, words, etc. representing and relating to a good or a service.

Interestingly, a trademark application need not be filed in respect of marks which are in use (but can also be filed in respect of marks which are intended to be used in the future). The primary requirements for registration of a trademark includes that it should consist of a mark capable of distinguishing the goods/services from those of others and that it is capable of graphical representation. The Trade Marks Act provides for absolute grounds of refusal of registration such as – (a) the mark not having a distinctive character; (b) a mark being deceptive and confusing to the public; (c) if a mark is hurtful to religious sentiments; (d) the mark is offensive, scandalous, or obscure, etc. In addition to the absolute grounds of refusal, the statute also provides for relative grounds of refusal of registration (viz. similarity with pre-existing marks).

Further, India is a signatory to the Madrid Protocol under which a trademark can be applied for and registered internationally. However, the prerequisite for filing and registering an international application (under the Madrid Protocol) in a foreign jurisdiction is that the mark needs to be first filed in India.

A protection afforded from a trademark registration is imperative as it protects the brand name, logo, sound, shape, etc., and distinctively identifies the goods/services to the brand bringing uniqueness to the mark. Also, the validity of a trademark registration is for an initial period of 10 (ten) years which can renewed perpetually for successive period of 10 years (subject to timely filing of renewal applications).

3. The Patents Act, 1970 ("Patents Act")

A 'Patent' is an intellectual property right which protects any new invention. It is an exclusive right that protects the rights of the inventor and prevents other people to unauthorizedly use and misappropriate the registered patent.

A patent is granted for a term of 20 (twenty) years from the date of filling of the application. It is important to note that patent for a new invention is registered only if the invention is 'novel' and 'original' i.e. it has not been introduced in the public domain in India or anywhere in the world; is 'capable of industrial application' which refers to the ability of the invention to be used in an industry; and is an invention that requires to employ a process of 'inventive steps', which is defined as 'a feature of an invention that involves technical advance as compared to the existing knowledge or having economic significance or both and that makes the invention not obvious to a person skilled in the art', under the Patents Act.

The Patents Act bestows each inventor, whose patent has been registered, with certain rights, namely:

- with respect to a patent for a product, the right to prevent third parties form using, selling, making, importing, etc. the product without prior consent; and
- with respect to a process for which a patent is obtained, the right to prevent third parties from using, selling, offering, etc. a product obtained from that process, without the prior consent of the original inventor.

Further, India is a signatory to the Patent Cooperation Treaty (PCT) which permits an applicant to file an application for registration of an international patent. Upon filing such application, an inventor can obtain patent protection in multiple countries (members of PCT), simultaneously.

4. The Design Act, 2000 ("Design Act")

A 'design' under the Designs Act [section 2(d)] means and includes 'only the features of shape, configuration, pattern, ornaments or composition of lines or colours, applied to any article whether in two dimensional or three dimensional or in both forms, by any industrial process or means, whether manual, mechanical or chemical, separate or combined, which in the finished article appeal to an are judged solely by the eye'.

An application for registration of an industrial design is to be made to the Controller- General of Patents, Designs and Trade Marks. However, a design shall only be considered for registration if – (a) it is novel and an original innovation i.e., it has not been produced before or reproduced by anyone; (b) it has not been disclosed to the public anywhere in India or outside the jurisdiction of India; and (c) it can be easily distinguished from other known designs.

Furthermore, once a design is registered, the registered proprietor is afforded protection for an initial period of 10 (ten) years, which is extendable (upon filing an application for extension) for a further period of 5 (five) years.

5. The Geographical Indications of Goods (Registration and Protection) Act, 1999 ("GI Act")

Many goods in India are widely popular owing to their place of origin. For instance, 'Darjeeling tea' is unique and popular owing to many factors including but not limited to its origin, the skill set of the tea farmers of Darjeeling and the weather prevailing in that area. Other such examples of products which have a bearing of the place of origin (or factors specific to the place of origin includes Banarsi Saree; Basmati Rice, etc).

A 'Geographical Indication' is defined as 'an indication which identifies such goods as agricultural goods, natural goods or manufactured goods as originating, or manufactured in the territory of country, or a region or locality in that territory, where a given quality, reputation or other characteristic of such goods is essentially attributable to its geographical origin and in case where such goods are manufactured goods one of the activities of either the production or of processing or preparation of the goods concerned takes place in such territory, region or locality as the case may be'. The GI Act covers only goods such as agricultural goods, food stuff, handicraft goods, manufactured goods, and natural goods.

An application for registering a good under the GI Act requires a statement explaining how the geographical indication affects to the origin of the good in terms of the quality, characteristics, and reputation of the good; the class of goods; particulars with regards the appearance of the geographical indication and the map of the territory/area/country where the good has originated.

A registered geographical indication is awarded protection for a term of ten (10) years with the option of renewing and extending such protection for further tenures of ten (10) years from the date of expiration of the original registration.

6. The Protection of Plant Varieties and Farmer's Rights Act, 2001 ("Plant Varieties Act")

The objective of the Protection of Plant Varieties and Farmer's Right Act, 2007, is to recognize rights of Indian farmers and to provide protection to plant varieties in order to encourage the growth and development of more plant varieties.

In 1994, India became a member to the Trade Related Aspect of Intellectual Property Rights Agreement (TRIPS) under which all members are required to accommodate and provide for the protection of plant varieties [Article 27(3)(b) of TRIPS]. All plant varieties that have been registered and awarded protection are entered and recorded into the National Register of Plant Varieties.

The Plant Varieties Act permits any breeder, farmer and any person as authorized, to apply for registration of a new plant variety. A new plant variety is registrable if it satisfies the conditions of 'novelty, distinctiveness, uniformity and stability'. To elaborate, the condition of novelty requires that at the date of filing the application (for protection), the plant variety must not be sold. Further, distinctiveness encompasses the requirement of having at least one distinguishing factor from all other existing and protected plant varieties. The requirement of uniformity means that all essential characteristics of the plant variety must be uniform. Lastly, the plant variety being registered for is required to be 'stable', meaning that the essential characteristics of the plant variety must remain unchanged after repeated propagation of such plant variety.

The validity of registration for the protection of a plant variety is for a period of nine (9) years in the case of trees and vines, and for a period of six (6) years in the case of crops, with the option of renewal of such registrations.

7. The Semiconductor Integrated Circuits Layout- Design Act, 2000 ("SICLD Act")

A 'semiconductor integrated circuit' is defined as 'a product having transistors and other circuitry elements which are inseparably formed on a semiconductor material or an insulating material or inside the semiconductor material and designed to perform an electronic circuitry function'.

Under the SICLD Act, all layout-designs capable of being registered are required to be original; commercially unexploited anywhere in India and in any convention countries; inherently distinctive and inherently distinguishable from other registered layout- designs. An application for registration of design layouts has to be in writing and is required to be filed before the Registrar in the Semiconductor Integrated Circuits Layout-Design Registry present in the territorial limits of the principal place of business of the applicant.

Further, the protection afforded to registered layout-designs is for a period of 10 (ten) years.

Conclusion

In India, there are different forms of intellectual property rights, allowing a person to obtain protection for their assets. India has actively become party to many conventions and treaties in order to afford international recognition and protection for intellectual property rights recognized in India. Some conventions have led India to introduce new enactments such as the Plant Variety Act, in order to award protection to goods that represent the heritage, agricultural background and fauna of India.

WHAT IS INTELLECTUAL PROPERTY TOOLKIT

Countries with innovative local industries almost invariably have laws to foster innovation by regulating the copying of inventions, identifying symbols, and creative expressions. These laws encompass four separate and distinct types of intangible property – namely, patents, trademarks, copyrights, and trade secrets, which collectively are referred to as "intellectual property."

PATENTS

- **Legislation**
  The Patent Act of 1983 and the Patent Regulations of 1986 govern patent protection in Malaysia. The purpose of the Act is to give legal protection to patent holders together with exclusive rights that include the exploitation of the patents, the assignment or transfer of rights, and license contract signature.
- **Revisions**
  The Act was revised in 1995 to speed up the processing and granting of patents in accordance with the Paris Convention and to extend the protection of patent rights. The Act was again revised in 2000 to extend coverage from 15 to 20 years; to incorporate Malaysia's accession to the multilateral TRIPS Agreement; to allow for parallel imports; and to limit the Government's power to exploit patents only during emergencies. The Act was revised most recently in 2003 to amend Section 35 on patent applications and to repeal Section 13.
- **Coverage**
  What does a patent protect?
  A patent is an exclusive right granted for an invention, which is a product or a process that provides a new way of doing something, or offers a new technical solution to a problem. Patentable inventions must possess the following characteristics:
    - They must be new, meaning that the invention has not been publicly disclosed in any form, anywhere in the world;
    - They must involve an inventive step, that is to say the invention must not be obvious to someone with knowledge and experience in the technological field of the invention;
    - They must be industrially applicable, meaning it can be made or used in any kind of industry.Non-patentable inventions include:
        - Discoveries, scientific theories, and mathematical methods;
        - Plant or animal varieties or essentially biological processes for the production of plants or animals, other than man-made living micro-organisms, micro-biological processes and the products of such micro-organism processes;
        - Schemes, rules or methods for doing business, performing purely mental acts or playing games;
        - Methods for the treatment of human or animal body by surgery or therapy, and diagnostic methods practiced on the human or animal body.

Inventors may apply for a utility innovation, which is an exclusive right granted for a "minor" invention that is not required to satisfy the same test as the patented invention.

The term of a patent is 20 years from the date of the filing of the application. The term for a utility innovation is 10 years from the date of filing, with the possibility of renewal for 5+5 years upon proof of use.

- **Registration**
  The Patent and Utility Innovation Administration and Examination Manual also provides useful information for the application process of a patent or utility innovation. Further questions about the registration process may be referred to the Malaysian Intellectual Property Corporation, MyIPO.
- **Infringement and Enforcement**
  The Patent Acts provide for patent enforcement by the Enforcement Division of the Ministry of Domestic Trade and Consumer Affairs. Patent owners shall lodge an official complaint supported by the necessary documents to the Ministry's Enforcement Division if they suspect infringement. The Division will conduct the necessary investigations and prosecutions. [Information above provided by the Malaysian Industrial Development Authority and the Malaysian Intellectual Property Corporation, MyIPO]

COPYRIGHT

- **Legislation**
  The Copyright Act of 1987 governs copyright protection in Malaysia. The Copyright Act provides comprehensive protection for copyrightable works. The act outlines the nature of works eligible for copyright, the scope of protection, and the manner in which the protection is accorded.
- **Coverage**
  What does copyright protect?
  The Copyright Act protects the following:
  - Literary works
  - Musical works
  - Artistic works
  - Films
  - Sound recordings
  - Broadcasts
  - Derivative works

  The copyright protection lasts for the author's lifetime and 50 years after his or her death. If a work has not been published during the lifetime of the author, copyright in the work subsists for 50 years. If the work has joint authorship, the life of the author who dies last is used to compute the copyright expiration.

  For sound recordings, copyright protection shall subsist for 50 years since the recording was first published. If the sound recording has not been published, the year of recording (?) is used to compute the duration of the copyright. For the copyright of broadcasts and films, protection also lasts 50 years.

The Copyright Act also provides protection for the performer's rights in a live performance, which subsists for 50 years from the beginning of the calendar year following the year in which the live performance was given.

What are the rights of copyright holders?
The copyright holder is initially the author of the work; however, if an employee makes the work during the course of his employment, the person who commissioned the work, unless there is any contrary agreement, holds the copyright. The author's right is also transferable.

Copyright holders generally hold the rights to control the following:

- Reproduction of the work in any form (photocopying, recording, etc.);
- Performing, showing, or playing the work to the public;
- Communication to the public;
- Distribution of copies to the public by sale or other transfer of ownership;
- Commercial rental to the public.

These rights apply whether the works are copied partially or wholly. Infringement occurs when a copyright holder can prove the defendant has violated any of these rights. Thus, the burden of proof lies on the person claiming that his or her work has been unlawfully copied.

- **Registration**
  There is no registration of copyright material in Malaysia. A work is automatically protected under the following conditions:
  - Sufficient effort has been made to make the work original in character;
  - The work has been placed in material form (written, recorded, etc.);
  - The author is a qualified person, the work is made in Malaysia, or the work is first published in Malaysia.

Infringement and Enforcement
A copyright work is infringed when a person who, not being the owner of the copyright, and without license from the owner, does or authorizes any of the following:

- Reproduces in any material form, performs, shows or plays or distributes to the public, communicates by cable or broadcast of the whole work or a substantial part thereof either in its original or derivative form.
- Imports any article into Malaysia for the purpose of trade or financial gains.
- Makes for sale or hire any infringing copy.
- Sells, lets for hire, or by way of trade, exposes or offers for sale or hire any infringing copy.
- Distributes infringing copies.
- Possesses, other than for private and domestic use, any infringing copy.
- By way of trade, exhibits in public any infringing copy.
- Imports into Malaysia, otherwise than for his private and domestic use, an infringing copy.

- Makes or has in his or her possession any contrivance used or intended to be used for the purpose of making infringing copies.
- Causes the work to be performed in public.

The Copyright Act of 1987 provides for copyright enforcement by the Enforcement Division of the Ministry of Domestic Trade and Consumer Affairs, apart from the police. Copyright owners may lodge an official complaint supported by the necessary documents to the Ministry's Enforcement Division if they suspect infringement. The Division will conduct the necessary investigations and prosecutions.

[Information above provided by the Malaysian Industrial Development Authority and the Malaysian Intellectual Property Corporation, MyIPO]

TRADEMARK

- **Legislation**
  The Trade Marks Act of 1976 and the Trade Marks Regulations of 1997 govern trademark protection in Malaysia. According to the MIDA, the Act provides protection for registered trademarks and service marks in Malaysia. Once registered, no person or enterprise other than its proprietor or authorized users may use them.
- **Coverage**
  What does trademark protect?
  A trademark is a sign that distinguishes the goods and services of one trader from those of another. A sign includes words, logos, pictures, names, letters, numbers or a combination of these.According to MyIPO, a trademark exhibits the following functions:
  - Origin Function – A trademark helps to identify the source and those responsible for the products and services sold in the market.
  - Choice Function – A trademark enables consumers to choose goods and services with ease while shopping.
  - Quality Function – Consumers choose a particular trademark for its known quality.
  - Marketing Function – Trademarks play an important role in advertising. Its normal for consumers to make purchases based on continuous influence of advertising.
  - Economic Function – Established trademark is a valuable asset. Trademark may be licensed or franchised.

  MyIPO lists the following items as eligible for trademark registration:

  - Invented word or words
  - Names of person, firm, or company mentioned in a specific manner
  - Applicant's signature
  - Words with no direct relation to goods or services, geographical name of surname
  - Any distinctive sign such as logos, pictures, symbols, etc.

Trademarks may not be deceptive or confusing, contrary to law, scandalous or offensive, identical or similar to earlier registered (or applied) trademarks, identical or similar to a well-known trademark.

Under Section 15 of the Trade Mark Act and Regulations 13, 14, and 15 of the Trade Mark Regulation, trademarks may not be registered if they include the following words:

- Patent, Patented, By Royal Letters Patent, Registered, Registered Design and Copyright;
- His Majesty Yang di-Pertuan Agong, Her Majesty Raja Permaisuri Agong, The Royal Highness Sultans and Their Excellencies Yang di-Pertua Negeri;
- Royal or Imperial Crowns, Arms, Crest, Armorial bearings or insignia;
- The Royal Malaysian Army and Royal Malaysian Police;
- Red Crescent, Geneva Cross in red and Swiss Federal Cross in white or silver on red ground;
- Words or representation of ASEAN and National Flower.

The term of protection is ten years for trademarks, renewable every ten years thereafter.

What are the rights of trademark holders?
Registered trademark owners have exclusive right to use their marks in trading. They also have the rights to take legal action for infringement under the Trade Mark Law against others who use their marks without consent. They can either take civil action or lodge complaints to Enforcement Division for appropriate actions under the Trade Description Act of 1972.

- **Registration**
  MyIPO diagrams the trademark application process
  According to MyIPO, every application will be examined to ensure whether the proposed trademark is eligible for registration. If there is an objection to the trademark, applicants may submit responses in writing or apply for a hearing. Trademarks accepted for registration will be advertised in the Government Gazette to allow any part to forward their opposition on the registration of the trademark. If there is no opposition, the mark will be registered and a Registration Certificate will be issued. The application fee is RM 250 as well as RM 450 for advertisement and issuance of certificate. (Total approximately: USD $187.00)
- **Infringement and Enforcement**
  The Trade Mark Act and Trade Mark Regulation provide for trademark enforcement by the Enforcement Division of the Ministry of Domestic Trade and Consumer Affairs. Trademark owners shall lodge an official complaint supported by the necessary documents to the Ministry's Enforcement Division if they suspect infringement. The Division will conduct the necessary investigations and prosecutions.
  [Information above provided by the Malaysian Industrial Development Authority and the Malaysian Intellectual Property Corporation, MyIPO]

Copyright Rights and Neighbouring rights

From many years entertainment has played a very significant role in human beings' lives be it movies, songs, Drama etc. All the forms of entertainment gained equal recognition and praise by their respective audience irrespective of the country or language they have had been or still being performed. As the time passed by event, the nature of the entertainment Industry has changed, before Independence the film used to be shot in black and white later with the time, and due to technology, the focus shifted from black and white to color films.

As the time of the entertainment industry was changing leaps and bounds the performers Actors, Singers, Lyricist, Music composers all of them started gaining popularity for their performances on screen or in the Background. Many people back then started mimicking their favorite performers, which performer's up to some extent use to like.

This popularity gained by the performers put them into larger risk of getting their work copied or as we call it getting their infringed. During that era there was no concept called "performers Rights" under Indian Copyright Law Actor's performance in the film or performance of singer with whose help the song written or composed was communicated to the audience were not protected. After many years of this inequality finally in the year 1994 the concept of performers rights was adopted in India.

Introduction:

The Indian copyright law has recognized two types of rights:

a. copyright
b. Related rights

Copyright refers to the right which is granted to Authors, artists and other creators in order to protect their work (Literary as well as artistic) on the other hand, the related rights also known as neighboring rights granted to those who are the technical authors of the work but has a significant amount of contribution towards the creation of the work.

For example, if A writes a song for T-series in exchange of the remuneration and royalties then, T-series becomes the Author and owner of the song, but A will still have few rights to protect his work with respect to performing such song to the public at large although not being an author anymore. These rights are called as "RELATED RIGHTS" under copyright law,1957. Basically, these rights deal with the rights of such persons who does not create the work instead, communicates such work by performing or broadcasting it to the public at large. Related right is generally used to showcase creativity or technical and organizational skill which justifies the recognition of a copyright like property in nature.

Apart from recognizing related rights such performers rights and broadcasting rights under Indian Copyright law, India also made himself a party to different legislation with respect to Related or Neighboring rights.

Those legislation are follows:

A. Berne Convention for the protection of Literary and Artistic Works, 1886.
B. Universal Copyright Convention.
C. Convention for the Protection of producers of Phonograms against unauthorized Duplication of their Phonograms, 1971.
D. Trade Related Aspects of Intellectual Property Rights (TRIPS) Agreement.1994.

As per the international conventions and WIPO related rights are bifurcated into three different beneficiaries:

1. **Broadcasting Rights:**
   this Right is related to broadcasters, who disseminate the said work through broadcasting through TV, Radio, Internet etc. According to the Indian Copyright law, the tenure for broadcasting rights is of 25 years and it has been mentioned under section 39 of the Copyright act, 1957 which states " No broadcast reproduction right or performer's right shall be deemed to be infringed by: "S 39. Acts not infringing broadcast reproduction right or performer's right. :No broadcast reproduction right or performer's right shall be deemed to be infringed by:

   a. the making of any sound recording or visual recording for the private use of the person making such recording, or solely for purposes of bona fide teaching or research; or
   b. the use, consistent with fair dealing, of excerpts of a performance or of a broadcast in the reporting of current events or for bona fide review, teaching or research; or
   c. such other acts, with any necessary adaptations and modifications, which do not constitute infringement of copyright under section 52". And over the years, this right has been proven to be the quickest way for exploiting the work by circumventing it through different means therefore, all the broadcasting organizations such as news channels, Radio channels possess these rights.

2. **Phonograms:**
   Another aspect of related rights is phonograms, Phonograms means an "Aural Fixation" (except for soundtracks, of films or video cassettes), whatever in form (disc, tape). The protection is provided for the years of 20 years which will start from the date of first fixation or the first publication of the phonogram whatsoever however, the protection granted by the domestic countries can eb extended up to 50 years.

   This right was recognized under the treaty of WPPT which was passed in the year 1996. These rights are most importantly granted to the producers of phonograms which have a completely right over the sound recording. Furthermore, no mentioned with regards to this protection has not been mentioned under the Indian Copyright Law, 1957 but since India adopted the legislation of WPPT, producers of phonograms are entitled for the protection.

3. **Performers:**
   the third most important part of the related rights are "Performers" the provisions of which has been elucidated in this article, India has recognized performers rights under the Indian Copyright (amendment) 1957, which was in consonance with the Rome Convention in the year 1961 and also the WPPT act, 1996 Performers are considered

as pivotal link between the performance and society. performers give their best to deliver the essence or theme of their artwork to the people but are often incapacitated when it comes to the protection of their work because copyright act does not expressly elucidate any such rights given to the performers in India until 1994 amendment under copyright law which could protect their work from infringement under their respective copyrights Act.

Now-a-days, due to globalization innumerable entertainment streaming platforms like you tube channels and diverse OTT platforms such as Spotify, amazon prime music, netflix have started evolving. People from all over the world who are fond of listening to music or who revere a particular performer as their icon, to state it ordinarily who claims themselves as their "fans" can enjoy their piece of work or art of work through such digital platforms, but is this process legal? People put up such work of the performer [1] on their you-tube channels without seeking the artists consent which ultimately results in infringement of performers right. In this Article we are going to study Related Rights also known as Neighboring Rights under copyright act 1957.

Performer's right is intrinsically associated with the "performer" whether it is a singer, actor, musician, dancer, acrobat, juggler, or even a person delivering a lecture (section 2(q) of the Indian copyright act,1957). However, there was no recognition given to such rights by the Indian copyright act,1957 till the act got amended in 1994, **Fortune Films V. Dev Anand** after which performers right were given recognition and were defined under section 38 of Indian copyright act, 1957:

Performer's Right:
Any engagement of a performer in any kind of performance renders him the right through which he can hold his own interest in the performance known as "performer right". Such right according to the rome convention,1961 and section 38 of copyright act 1957 subsists for 20 years from the beginning of the calendar year to the next following year with-respect to the date on which such performance was made. Furthermore, in continuance of these rights in respect of any performance if a person continues to do following acts without the consent of the said performer:

a. Reproduces a sound recording or visual recording of the performance which has been:
    i. Made without the consent of the performer;
    ii. Made for the purposes which are different from those for which the performer has given his consent;
    iii. Made for purposes which are different from those purposes referred in sec 39 from sound recording or visual recording which was created in consonance with S. 39 which states (acts not constituting infringement);
b. secondly, if there is a Broadcasting of the performance except where such broadcast is made from a particular sound or visual recording other than those made in parlance with S. 39 or which are rebroadcasted by the same broadcasting organization of an earlier broadcast which did not infringe the right of a performer.
c. thirdly, renders such performance to the public at large otherwise than by broadcast except, wherein such communication to the public is made from sound recording or a visual recording or a broadcast.[2]

Why performers right should be protected?

Earlier performers right never received that kind of recognition as there were no digital platforms to disseminate such work and even there were no such technological developments therefore people use to go live to watch the performance and no fixation of the performance was possible so performer was obliged to repeat his performance as and when required but, today since technological developments are touching skies it became very easy to circumvent performers work (performance) digitally through recording or even by means of broadcasting and exploit such work commercially to reap profits, and also made it easy to fix a live performance.

Artists or performer try to deliver their best out of their compositions or performance, so that they could measure up to the audience expectations. Rapid growth in modern technology made it facile to record such performances or broadcast them without seeking performers consent for commercial purposes which ultimately increases the economic value of that work resulting in huge number of profits to the broadcasting company or sound recording company whilst performers are entitled to a certain amount from those profits for their work which perhaps wouldn't be of much a worth.

To avoid such instances and to acquire appropriate compensation or rewards for their work performers rights were enshrined under the statute, so that performers could gain the kind of recognition they deserve which was earlier use to get overshadowed by the broadcasting and sound recording companies. Development of such rights laid down specific procedure and authorities to deal with sound recording of the performance or even broadcasting of such performance on radio or television, eventually increasing the labor opportunities.

International Conventions:

Apart from the Copyright Act, the international convention for broadcasting organizations generally known as Rome convention, 1961 became the first convention to recognize performer rights along with international labor organization and mainly, the World Intellectual Property Organization (WIPO) .

The protection laid down by the Rome convention for the protection of performer's right is 20 years from the fixation of the work created Similarly Article 19 of the Rome convention elucidates "if any performer has agreed for the incorporation of his work through agreement or contract in any audio-visual form or visual form then in such scenario the provisions related to performer's right (Article 7) will not be applicable to the performer."

Rights Of Performers Under Rome Convention:

Article 7 talks about the rights acquired by the performers under the Rome convention they are:

1. Right to prevent others from non-consensual broadcasting or communicating of the performance except otherwise where, the performance is already a broadcasted performance or is made from fixation.
2. Right to prevent others from fixing a price for the performance without their consent or for performance which is made for different purpose rather than the one for which the performer consented for and wherein the original fixation is made inconsonance with A. 15 and the reproduction of the same differs from those provisions mentioned in the same.
3. Right to prevent from commercial exploitation of their work when consent is not obtained from them.[3]

WPPT (WIPO PERFORMANCE AND PHONOGRAMS TREATY, 1996)[4]

Another convention which elucidates rights pertaining to the performers for their work purely fixed in the phonograms is WPPT which was established 1996 in Geneva, and which more importantly extended the rights which can include licensing. Right to reproduction (Article7), "Right of Distribution" (Article8), "Right of rental (Article 9)" and "Right of availability of fixed performances (Article 10)".

a. Article 7- performers can avail this exclusive right wherein they get the power to authorize the reproduction of their performances fixed in phonograms or any other medium.
b. Article 8- this article empowers the performers to distribute their work in public either originally or copies thereof through sale or transfer of ownership.
c. Article 9- This right Empowers performers to rent his/her performance to public either original or copies thereof in consonance with the national laws of the contracting parties
d. Article 10: By Accessing this Right, performers can disseminate their performance by wire or wireless means in such a medium where public can get access to it at a time and place chosen and suitable for them.[5] As Provisions of This convention were purely subjected to the performer's performance exclusively fixed in phonograms and not in audio-visual performances this was the time Beijing treaty came into picture

The Beijing Treaty was established to regulate audio-visual performances eventually, expanding the rights of the performers. This treaty was signed on 24th June 2012 but never came into force until it was finally ratified by 30 eligible parties, ultimately, coming into force on April 20th, 2020. This Multilateral treaty Acknowledged, the intellectual property of the performer's performance in audio-visual works internationally eliminating the discrimination between sound performances and Audio-visual performances laying down a strong foundation that all performers are entitled to the intellectual property Rights Protection regardless of the fact how they are been delivered.

Copyright Act 2012 Amendment

Copyright Act 1957, again got amended in 2012 which was in compliance with the WIPO Performers and phonograms treaty, 1996 also known as WPPT and the Beijing Treaty 2012,

which explicitly provided the performers with the following rights under section 38A and 38B of the Copyright (Amendment) Act,1957 and in addition to that, this amendment also entrusted the right to receive royalties in case if such work has been used for commercial purposes.

Say for instance, if a Dungeon & dragons Productions intends to put a particular song in the movie which was originally made in different language, then, here the performer who has performed such piece of work will be entitled to get royalties from dungeons & dragon productions for that song.

Exclusive rights for performers

Without being prejudicial to the Rights granted to the Authors by the Copyright Act 1957, performer Rights is an exclusive Right which permits to execute following acts with respect to performance or any substantial part thereof under Section 38A of the Copyright (Amendment) Act
namely:

a. to make a sound recording or a visual recording of the performance, including-reproduction of it in any material form including the storing of it in any medium by electronic or any other means; (Right to Reproduction)
b. issuance of copies of it to the public not being copies already in circulation; (Right to distribution)
c. communication of it to the public
d. selling or giving it on rental basis or offering it for sale or in case of commercial rental any copy of the recording; (Right of Rental)
e. to broadcast or communicate the performance to the public except where the performance is already broadcast.

(2) Once a performer, by a written agreement, gives his consent for incorporation of his performance in a particular cinematograph film he shall not be opposed by the producer of the film from enjoying his performer's right in the same film, provided that, notwithstanding anything contained in this sub-section, the performer shall be entitled for royalties in case of making of the performances for commercial.

The performer's right would be at par with the rights of the producers/music composers once the performer through an agreement willingly agrees to subsume his piece of work in a film and then the producer would be entitled to gain economic benefits through the commercial use of the performance and the producer in any way cant preclude the performer from rendering the adequate amou0nt of royalties for commercially exploiting his (performers) work. Furthermore, if the performers work is being communicated to the public or society other than films e.g., live performance even in this case the performer will gain royalties for his work as these rights are unassignable in nature. Yet, another Section 38B of Copyright ACT,1957 which was inserted after the 2012 amendment extended moral rights to the performers in case of any infringement by any other person. As the name (Moral Rights) itself exemplify, the Rights which are non-economic they are more of performer's personal

rights attached with his/her creation or performance.

Section 38B: [7]
The Performer of performance shall, independently of his Rights after assignment, either wholly or partially of his Right, have the Right:

a. To claim to be identified as a performer (Article 5 WPPT 1996: moral right)
b. Restrain or claim damages in respect of any distortion, mutilation, or any other modification of his performance Which is prejudicial to his/her reputation. (Article 5 of WPPT Moral right)

Notwithstanding the provisions of section 38B of Copyright Act 1957 & according to the amendment of 2012 of the Copyright Act there are certain exceptions with-respect to section 38B(2), which states that if any portion of the performance or recording undergoes editing due to some technicalities such as: the duration of the recording, such reasons cannot be deemed prejudicial to the performers reputation thereby, absolving the provisions laid down in Section 38B(2).

Case Laws:
[8]Neha Bhasin Vs Anand Raj Anand
Facts
"Facts of the case were, the defendant hired the sound engineer for mixing the music with regards to the film "ARYAN-UNBREAKABLE" around January, 2006. One of the songs that the sound engineer was engaged to make it a remix was named as "EK LOOK EK LOOK". The engineer here, was handed over with the two recordings which was copies of the master recording of the song as per the instructions of the defendant.

The instructions given by the defendant further mentioned the name of the lead vocalist as "Poonam Khubani" and the name of "Neha Bhasin" as the back up vocalist. In the Inlay cards of CDS that were sold in the market, the plaintiff was shown only as a backup artist whereas Poonam Khubani was shown as the main lead vocalist.

Neha Bhasin, the plaintiff of the case, contended that she was called by the defendant for the recording of the song "EK LOOK EK LOOK" and she was the main lead vocalist of the song and Poonam Khubani was given false credit for having sung the song as a main lead vocalist whereas, it is the song sung in the plaintiff's voice which has reached the public. Plaintiff came to know about this when she saw the song on the television she confirmed the same on the purchase of a cassette and an audio CD. And sent a notice was sent to defendants

The particulars of the notice mentioned:

a. That though Plaintiff had auditioned with defendant No 1 for the concerned song, the defendant No 1 decided to use the voice of defendant No 2 for the said song.
b. Plaintiff Voice got mixed up with defendant No 2 voice by the sound engineer inadvertently

c. This inadvertence was carried to the printer and that's why the name of plaintiff was on Inlay Card
d. As soon as this was brought to notice of defendant No 1, the sound engineer was asked to rectify the mistake
e. All the next lot of CD's and cassettes have been postponed and all the material being recalled
f. With the above mentioned claims the petitioner also sought an apology from the defendants.

Issues:

1. Was defendant no 2 the lead singer of the song?
2. Was layering a valid defense by the defendants?
3. performers right only subsist in live performances.
4. was there a contract between the party.

Contentions
Plaintiff's Contentions:

1. the Petitioner contented that she was approached through her manager when she agreed to sing for him for which no remuneration was paid to the plaintiff, prior to the first recording post which few more recordings were taken place along with the Rap piece.
2. All the three versions are in Plaintiff's voice and defendant no 2 is not the main singer. Plaintiff voice has been stolen and has been falsely claimed to be that of defendant no 2.
3. Moreover, the petitioner also contented that, this act of defendant has violated the performer rights of the petitioner under section 38 of the copyright Act 1957, and also as per the provisions laid down under the Rome convention.

Defendants' contentions:

1. the Defendant's solely relied on the defense of layering, wherein they stated that the voice of defendant no 2 was "layered" to that of the plaintiff
2. such layering projected defendant no 2 as the lead singer of the song in the film.
3. Because of this layering defendant No 2 was claimed to be the lead singer of the song and the plaintiff was claimed to be the backup vocalist.
4. The defendant contended that, the version of the plaintiff has been removed and have been replaced with the voice of the defendant and all the CDs are being recalled.

Judgement:

- An ex-parte order was passed by the high court of Delhi against the defendant and restrained them from Using, selling, distributing, exhibiting the motion picture as well as audio cassettes, compact discs, promos of the said film containing the song EK LOOK EK LOOK without highlighting the name of the plaintiff as the lead singer.

- Furthermore, the court was of the opinion that, "Every performance has to be live in first instance whether it is before an audience or in a studio" if this performance is recorded and thereafter exploited without the permission of the performer then the performers right is Infringed

United Kingdom Perspective:

Earlier, there was no recognition of performers rights in the United Kingdom, till 1911 act the performers rights was being neglected just like India until the 1994 amendment. In 1925, United Kingdom made an attempt to protect the performers rights, it was in the year 1925 when the government of United Kingdom made performers rights and criminal offence by introducing the "Dramatic and Musical Performers Act, 1925" but did not granted civil protection to the performers this was put forward into test in the case of Musical Performers Protection vs British international Pictures Ltd. (Blackmail case).

In this case, the George committee was of the opinion that performer rights are not eligible for civil protection moreover the George committee also rejected the proposal made by the Musicians Union and variety Artistes federation which states that performers should be entitled a right which would be of same nature as that od copyright, which was rejected by the committee by passing an order that it wont be possible to extend the scope of copyright to performers and undesirable to give performers the right. Therefore, the Copyright Act, 1956 was passed by the legislature of United Kingdom. Which rendered civil rights on performers.

The debate for the protection for performer rights in United Kingdom went on for years, until 1988, the year which changed the perspective of the legislature with regards to the performer's rights in United Kingdom. through the case of RICKLESS vs UNITED ARTISTS CORP which changed the dynamics of the protection of performer rights in the United Kingdom.

Rickless v/s United Artists Corp

Facts

In this case, the defendant's wanted to make a sixth installment of the movie titled "The Trail of the Pink Panther" by using clips and out-takes of the scenes from the last 5 movies which was performed by the late actor "peter Sellers" in earlier pink panther movies. The plaintiff contended that the rights of the performance of the late Peter Sellers vests with the him, and the defendants are bound to take the rights from the actors executors for execution of the film.

Analysis

While deciding the case, the court placed an reliance upon the 1958 Act,

a. whether the act provides performers civil remedies for breach of statutory duty or whether it restricts its scope to the criminal remedies.
b. Whether the Act provides the reproduction of a performance without the permission of the performer after death is illegal.

Initially, the Court placed a balance of convenience, in the favor of Plaintiffs on both the above-mentioned questions and entrusted the damages in the amount of US $1 million. The defendants made an appeal to the high court. And claimed that section 2 of the 1958 (as amendment 1963) act does not confer a civil right on the plaintiff.

Judgement

In this Judgement, Sir Nicolas Browne Wilkinson opined. "The section elucidated In the act especially renders criminal offence. Nevertheless, In some circumstances, it can also confer private rights under the civil law. The judge concluded that the 1958 Act, does render a civil right of action to the plaintiff and the movie "the trail of the Pink Panther" constitutes a breach of these rights. Furthermore, was dismissed by confirming that Section 2 gives civil actions along with the criminal penalties.

Suggestion:

In my opinion, Neighboring Rights granted to the performers, broadcaster and producers of phonograms are of vital importance as they protect the inherent interest of the performers or broadcasters. Furthermore, any infringement of such rights by any person might result into severe punishment civil as well criminal wherein respective damages can be awarded by the court. In my opinion although there are regulations under the statute yet, there are infringements with respect to the performance performed by the performers.

For example, Taylor swift case in the United States of America, when "Taylor Swift" was precluded from singing her own song by the Music Label Big Machine Records on stage during her US tour likewise in India, the above-mentioned case mentions the clear case of performer rights.

In India, despite having a regulation performers works are subjected to infringements this is because performers are still not aware about their rights because of which all the record labels pressure the artists or performers and try to exploit their work in order to reap profits. To overcome this problem the performers should be very diligent when it comes to negotiating with the record labels and also when it comes to any contractual obligations, because these intricacies of the contracts come with a high price.

One of the main issues with regards to these contractual obligations is MSA (Master Service Agreement). When the performer signs this agreement, he waves off all the rights with regards to the song and all the rights vests with the record label for eternity and record label can make money by exploiting such work.

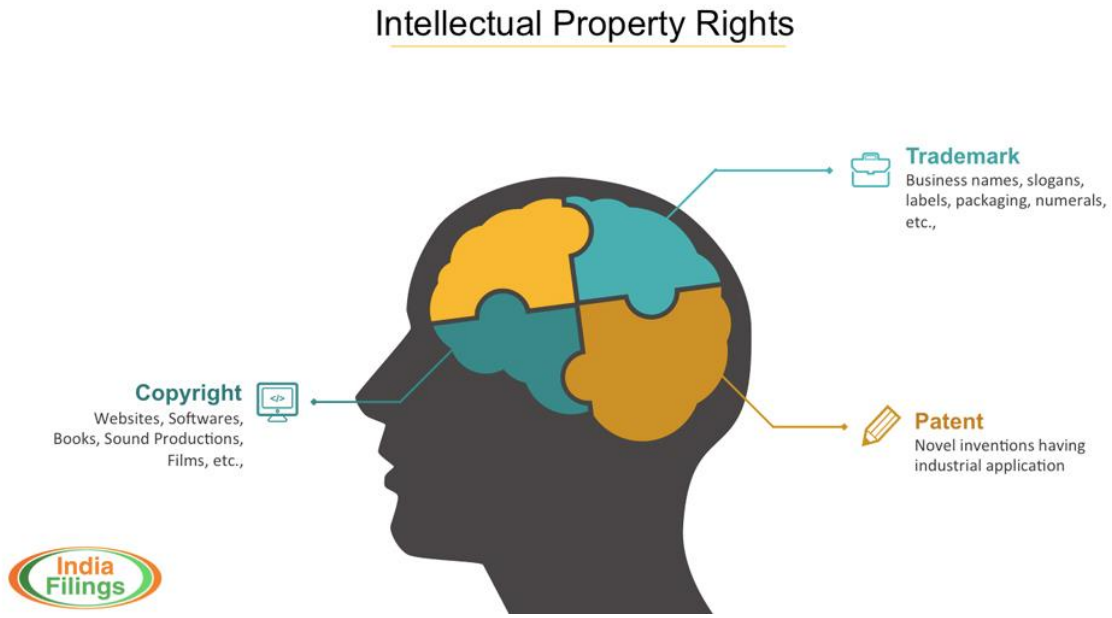
Conclusion:

In my opinion, everything that emanates from Human Mind or intellect whether it may be an artistic work, or a literary work has its own value which cannot be forsaken. Performer who develops any piece of work or renders performance has got his own integrity which cannot be put out on stake, and this was perceived very well by the authorities of India and hence, new section were incorporated under the Copyright Act, 1957 which gave allied rights to the performers, Broadcaster and phonograms producer to protect their work from infringement or mutilation by any third parties.

After contemplating all the above points, we can say that `just like other countries even India was very diligent when it comes to protection of their respective performers and looking at the growth of the music industry globally all these provisions will strongly help the performers to understand as well as protect the rights with respect to their performance.

Intellectual Property Rights Registration

In India, the intellectual property rights pertaining to trademarks and patents are controlled by the **Controller General of Patents Designs and Trademarks**, Department of Industrial Policy and Promotion, Ministry of Commerce and Industry. Copyrights are handled by the **Copyright Office**, Copyright Societies, Government of India. Based on the type of intellectual property right to be registered, application must be made to the concerned authorities in the prescribed form.



Intellectual Property Rights Overview

Trademark Registration

Trademark is the most common type of intellectual property right with more than 2 lakh trademark registration applications filed in India during the year 2013-14. Trademark registration and trademark protection in India are governed by the **Trademark Act, 1999**. A trademark is used by an entity on goods or services or other articles of commerce to distinguish it from other similar goods or services originating from a different entity. Names, logo, slogans, word signature, label, device (product shape), numerals or even a combination of colors can be trademarked in India. However, the most popular form of trademark registration is that of a trademark registration for a business name or logo. Once the trademark registration application is filed with the Registrar of Trademarks, the TM symbol can be used next to the logo. Once, the trademark is registered, the R symbol is placed next to the logo for indicating that the mark is a registered.

For a mark to be trademarked, it must be:

- Capable of being represented graphically (that is in the paper form).
- Capable of distinguishing the goods or services of one entity from those of others.
- Capable of being used or proposed to be used as a mark in relation to goods or services to indicate a connection between the goods or services and an entity that has the right to use the mark.

T= Copyright Registration

Copyright registrations are handled by the Copyright Office acting under the **Indian Copyright Act, 1957**. Copyright is a legal right given by the law to creators of literary, dramatic, musical and artistic works and producers of cinematograph films and sound recordings. Unlike trademark and patent, copyright protects the expression and not the idea or creation of mind. Further, copyright registration cannot be obtained for titles or names, short word combinations, slogans, short phrases – as the same can only be trademarked. One of the most popular type of copyright registration in India is copyright registration of website or software. Websites and software's can be copyrighted as they are both considered to be "literary works" under the **Indian Copyright Act, 1957**. To copyright a website, many separate applications for copyright registration may have to be filed, as a website could contain many different literary works, artistic works (photographs etc.), sound recordings, video clips, cinematograph films, broadcastings and computer software. For copyright registration of a software, the "Source Code" of the software must be submitted to the Copyright Office along with the application for registration of copyright for software products.

Patent Registration

Patent registration in India can be obtained for any invention relating to a product or process that is new, involving inventive step and capable of industrial application. The following items cannot be patented, as they are not considered as inventions under the **Patent Act, 1970**:

- An invention which is frivolous or which claims anything obviously contrary to well established natural laws.

- An invention the primary or intended use or commercial exploitation of which could be contrary to public order or morality or which causes serious prejudice to human, animal or plant life or health or to the environment.
- The mere discovery of a scientific principle or the formulation of an abstract theory or discovery of any living thing or non-living substance occurring in nature.
- The mere discovery of a new form of a known substance which does not result in the enhancement of the known efficacy of that substance or the mere discovery of any new property or new use for a known substance or of the mere use of a known process, machine or apparatus unless such known process results in a new product or employs at least one new reactant.

- Any substance obtained by a mere admixture resulting only in the aggregation of the properties of the components thereof or a process for producing such substance.
- The mere arrangement or re-arrangement or duplication of known devices each functioning independently of one another in a known way.
- Any method of agriculture or horticulture.
- Any process for the medicinal, surgical, curative, prophylactic diagnostic, therapeutic or other treatment of human beings or any process for a similar treatment of animals to render them free of disease or to increase their economic value or that of their products.
- Plants and animals in whole or any part thereof other than micro organisms but including seeds, varieties and species and essentially biological processes for production or propagation of plants and animals.
- A mathematical or business method or a computer programme *per se* or algorithms.
- A literary, dramatic, musical or artistic work or any other aesthetic creation whatsoever including cinematographic works and television productions.
- A mere scheme or rule or method of performing mental act or method of playing game.
- A presentation of information.
- Topography of integrated circuits.
- An invention which in effect, is traditional knowledge or which is an aggregation or duplication of known properties of traditionally known component or components.

Application for patent registration must be made to the Indian Patent Office in the prescribed format. A patent application can be filed either by true and first inventor or his assignee, either alone or jointly with any other person. It is important to remember that the application for patent should be filed before the publication of the invention and till then it should not be disclosed or published. Disclosure of invention by publication before filing of the patent application may be detrimental to novelty of the invention as it may no longer be considered novel due to such publication. However, under certain conditions, there is grace period of 12 months for filing application even after publication.

Emerging trends in Intellectual Property Rights

Changing trends in Intellectual Property

Intellectual property has seen various refinements in recent times. The 21st century is the century of innovation and creation and also is an era of the IP revolution. This era has the power to convert ideas and knowledge into wealth for the social good.

The huge difference that IPR has brought, which is necessary in recent times justifies what Victor Hugo said in a speech and I quote “no power on earth can stop an idea whose time has come.” This current era is bringing in various new types of Intellectual property rights in the field of technology, medicine, investments, and literary works.

Technology today is the answer to all the questions. It not only helps us in keeping touch with people globally but has also opened up doors for infinity of information in just one fingertip. But with great power comes great responsibility and that’s what exactly the laws today lack. Law is the answer to all the social and political issues and when law and technology come together, we get what we call as Copyright law.

The basic objective of Copyright law is to fix the authority of the inventor and the general user of the copyrighted work. In India, the software i.e. computer programmes is protected under Indian Copyright Act 1957. To achieve this objective copyright law has been amended globally various times.

IPR and Technology law is the major part of any business dispute or transaction and thus making it necessary, as any company big or small, wants to protect their innovations, ideas, design, products etc Strong IPR protection also has always been beneficial as they create revenue for the inventors and also the stakeholders.

Digitization of law has severely changed the format of how people used to work traditionally. Access of numerous information on internet has made the processing, distribution and execution of protected works much easy, but on the other hand availability of low-cost illegal copies and illicit use of copyrighted work has also taken a new high.

To protect the intellects from such threats Digital Rights Management (DRM) has added new measures to minimise the copying of original work without the owner's knowledge. Techniques such as Access Control and Copy control make sure that the creator of software can keep the check on users of his/ her products and it also ensures that the services are available ton only those who pay for it.

It also prevents any other party from getting a copy of the original work unless they have a license. A digital watermark is another technique that makes sure the creator is able to digitally track the unauthorized user of their work. The watermark embedded on the work can easily track illicit use. Encryption schemes also allow the creator to prevent any illegal access and only the decrypted user of work has the key to their work.

Pharmaceutical industries are offered exclusive rights to sell, import, and export drugs through Patents. The Patent prevents the other pharma companies to sell the drugs manufactured by those companies for next 20 years. IPR has the greatest impact on pharmaceutical companies, from manufacturing to pricing and then to distribution.

The year 2020 and 2021 were a huge challenge for the pharmaceutical industry as we were in the middle of a global pandemic. The pandemic essentials such as masks, disinfectants, hand sanitizers and PPE kits were widely in circulations during this period and is still in the market. With strong IPR several countries around the globe the pharma industry is growing in rapid speed and for the countries witch critical patent access the present market leads to monopoly resulting in increased prices of drugs.

But in the middle of a global pandemic the biggest challenge for us was not the access of vaccine and other health essentials but the question was how to identify the approved vaccine. There were various barrier that we faced with respect to access like lack of raw materials, lack of funds, lack of manufacturing departments and lack to access of innovations, ideas and knowledge in health sector.

The knowledge of Intellectual property right today was more important than ever. The researchers, the scientists all rely on patents to preserve their ideas and inventions from being stolen thus helping to build up the economy. The government along with private sectors helped in increasing the investment in medical and pharmaceutical research and innovation and also

made sure to reward those who put up their hard work to make the medical sector better than ever.

The government around the globe made sure that companies registered under Intellectual property rights should be benefited and funded. But in the present times we have to make sure that Intellectual Property right is not a barrier to the access of medical treatments and vaccines. It is rather a shield to make sure that every individual gets access to best treatments and cures which are medically proven.

But at the present case we are suffering from global innovation crisis and the funds required for innovations. Given the drastic suffering that we are going through with human health and welfare the world needs to make all the equipment required for innovations accessible.

Today, the biggest financial and legal asset that the companies and start-ups have is Intellectual property. The protection of a brand is done by trademark law on the basis of performance of company. Also, the companies with protected Intellectual property and investments are taken seriously in the market thus attracting higher quality partners and bigger investments.

The idea of Intellectual Property Rights also functions as a marketing tool and increase the value of business. The patent or the trademark sign on the product indicates the uniqueness of its and stands for its individuality and how it is different from all the other products available in the market.

Indian government, in order to showcase the innovative side of its country came up with schemes like Make in India in 2014 and Skill India in 2015. These two were the national platform designed to generate investment and bring out the innovative side of people in the country.

Conclusion

Thus, it is safe to say that in recent times of globally highly digital landscape, Intellectual Property Rights are most essential than it has ever been. IPR has given worth to the ideas and has made them commercially potential. Without taking adequate measures to protect one's invention or business, the individual can never reap the benefits of their hard-work.

The registration and patents of latest developments and innovations are also adding to the economy of the nation. With the rise of patents and trademarks of companies being shared on internet widely it has become easy for the people to illegally copy the ideas shared online but there are several counties who recognise the importance of original work and ideas and thus have very strict legal provisions for the same.

Industries such as medical and digital are at their peak at this moment, especially after pandemic and it has finally made the intellects and creators realise the importance of data protection and IP enforcements.

Uses of IPR

Intellectual property refers to any new idea or invention created by an individual or a business. It is essentially an invention that has both commercial and moral value. Such inventions that are new, innovative and life-changing can be protected by the individual who came up with the concept or product under intellectual property rights and laws that govern the country. Under

Intellectual Property Rights (IPRS), the inventor can get copyrights, patents, design and, trademarks and trade secret protection to shield an invention/creation from being duplicated or copied by another individual or business. In this article, we shall shed light on the benefits of intellectual property rights.

IPR benefits

There are five major advantages of intellectual property rights. They are as under:

- **IPRs can help turn your ideas into money-makers**
  Every little or big idea you have, can prove invaluable if it is executed correctly. This simply means that your intellectual property can help you convert your ideas into products and services which are commercially successful. You can use your intellectual property to create a business on your own, pitch it to investors and start a business or even get it licensed, enabling you to sell it to various businesses in exchange for a steady stream of income. An IPR can be converted into an asset and can help turn your idea into a huge money-maker.
- **IPRs can enhance your business' market value**
  One of the greatest advantages of protecting intellectual property is that it can generate income for your business in many ways. You could license your IP and lend it to various businesses in exchange for a fixed income or reasonable royalties. You could also reap benefits from selling your IP products and services for a fixed amount. Selling your IP can raise your profits and even improve your market share. Also, in case you sell your company or enter an acquisition or merger with another, registered and protected intellectual property assets can significantly enhance your business' value.
- **IPRs can help you stand out from the competition**
  Customers are always looking for something new and exciting. Every company aspires to be the first one to offer a breakthrough product to customers. If you wish to create a certain image for your business then IPs are absolutely essential. Remember, customers associate a certain value with their favourite brands. This is where factors like goodwill, trademarks, designs and logos come into the picture. Customers recognize brands from these factors and IPRs helps businesses differentiate their products and services within a market, while promoting them to its target customers.
- **IPRs can be accessed to raise finances**
  Another benefit of intellectual property ownership is that you can easily monetize your IP assets when you need to raise funds. You could choose to sell the IP, license it, or even use it as collateral while taking on a debt. Also, the government of India has created several laws that allow IP owners to use their IPs to their advantage while applying for any government or public funding including loans, subsidies and grants.
- **IPRs can enhance opportunities related to exports in business**
  IPRs give you the freedom to tread into the export business as well. There is no law that states that IPs need to be protected and can be used to benefit one within specific borders. With the help of IPRs you can use your designs and brands to market your products and services in foreign lands as well, thus improving your export prospects. You can seek franchising agreements with foreign companies and even export patented products.

So if you have a great idea, don't be afraid to convert it into a business. Understand your IPRS and keep the benefits of intellectual property rights in mind while doing the same

Misuse of IPR or Abuse of Intellectual Property Rights

Intellectual property abuse, basically, is a defence for a suit of IP infringement. When such defence proves to be justified in a case, then the defendant is spared from the liability of granting immediate relief to the plaintiff. However, the misuse doctrine does not prevent the party to rely on the courts in case of any future infringement. The intellectual property owners may return to court once they have "purged" the misuse, for example, by striking anti-competitive provisions in their licensing agreements.

A transparent and somewhat definite legal and judicial take on the abuse of intellectual property rights has largely remained limited to patent misuse, later extending to copyright misuse, which branched out of the former.

Both trademark and trade secret misuse are still subjects of academic debate and lack any practical application in courts.

Different forms of Intellectual Property Rights abuse have been elaborated under the following heads:

Patent misuse

At times, patent owner wrongfully uses the patent surpassing its legitimate scope. Patent misuse is the unjustified use of the acquired patent rights. Examples of patent misuse include illegal tying of products and services to the patented invention, price fixing, fraudulently making the customers pay royalties on items the patent of which has expired, and the like.

The concept of patent misuse first surfaced in the case of ***Adams v Burke***, decided by the US Supreme Court in 1873. The court held that after the first authorized sale of a patent product by the patentee, the product becomes the complete property of the purchaser, rendering the patentee devoid of his monopoly rights over the product. Subsequent purchasers acquire the same rights over the product as the seller had, and may use it in the same way the owner could have used. This came to be known as the **exhaustion doctrine.**

However, in the 19th century, not many facets of patent misuse were acknowledged by the judges. In the famous case of ***Henry v. A.B. Dick Co,*** the United States Supreme Court upheld the validity of licensing the use of tied or other related products along with the originally patented product. Usually known as the **Inherency doctrine**, this theory states that it was the inherent right of a patent owner, in lieu of his having exclusive rights over his product, to exercise the right to license the product on any terms and conditions he chose.

In 1917, the United States Supreme Court overruled the *A.B. Dick* case in ***Motion Picture Patents Co. v. Universal Film Mfg. Co.*** In this case the Supreme Court held that 'the scope of every patent is limited to the invention described in the claims. The patentee can claim nothing beyond them.' It condemned the licensing of materials which formed no part of the patented invention and were merely necessary for its operation.

In Brulotte v. Thys Co. (1964), the United States Supreme Court held that a patent holder's attempt to collect royalties beyond the term of the patent constitutes misuse of the patent.

An essential condition for using patent misuse defence is that it must hamper the competition in the market.

When a company accuses a patent owner of misuse, then the allegation must fulfill 2 conditions:

- The valid patent was used as a way to change business outcomes
- The anti-competitive effects extended outside of the patent's scope

The patent misuse doctrine requires that the alleged infringer show that the patentee has impermissibly broadened the 'physical or temporal scope' of the patent grant with anticompetitive effect. Patent misuse does not affect a patent's validity.

Since the 20th century, there have been significant developments through various legislations and judicial decisions that have further broadened the scope and understanding of the patent systems so as to eliminate the loopholes and make it more user- friendly.

Copyright misuse

Copyright misuse occurs when a company or an individual makes unjustified use of a copyright which is beyond its legal capacity and in violation of the Copyright Act of the concerned country. A copyright owner could commit misuse by violating any public policy choices embodied in the Copyright Act, such as by using a license agreement to extend the length of its copyright monopoly. Copyright misuse can also occur when the assertion of copyright is aimed at suppressing speech.

It is believed that Copyright misuse derives its basis from patent misuse as, while patent abuse finds mention in various cases since the 19th century, copyright misuse found recognition in the legal fraternity only a few decades ago.

Morton Salt Co. v. GS. Suppiger (1942) case, decided by the United States Supreme Court, laid the foundation of the concept of copyright misuse. While the reasoning given by the court refers to patent misuse, the commentary and the dicta address the issue of copyright misuse.

In *Alcatel U.S.A., Inc. v. DGI Technologies (1999),* it was held that the defense of copyright misuse has its historical roots in the *unclean hands doctrine*, i.e, which means that the suit of infringement filed by the plaintiff, who himself has abused the privilege conferred upon him by the copyright, is not itself justified. In the instant case, the Court found copyright misuse where the holder of a copyright in software licensed its use on the condition that the licensee also use it only in conjunction with the copyright holder's hardware. It prescribed the use of the copyright to secure an exclusive right or monopoly, which is not granted by the Copyright Office of a country and which is contrary to public policy to grant.

Upon the improper use of a copyrighted work, the work will provide no copyright rights to its owner. In order to retain the rights, it is important that the activity constituting the misuse must be ceased.

In the case ***Tekla Corporation v. Survo Ghosh***, decided by the Delhi High Court on 16th May 2014, Justice Endlaw of the Delhi High Court held that "copyright misuse does not constitute a legitimate defense for copyright infringement in India."

Patent trolls

Patent Trolls, formally known as 'Non-Practicing Entities (NPEs) or Patent Assertion Entities (PAEs)', are companies which tend to earn a fortune from frivolous patent infringement lawsuits. While normal companies use their patents to protect their product from being counterfeited and sold in the market, patent trolls often acquire patents cheaply from bankrupt companies and, instead of using such patents in operations, these companies charge hefty licensing fees on other persons or businesses which appear to infringe any of their acquired patents.

Fees can range from ten to hundred thousand dollars, whereas patent lawsuits can cost the individuals or companies in millions. Hence, when such are the costs, many companies prefer to concede and settle, even if they believe there to be no patent infringement.

This practice is a lucrative option for making money with minimal risks. Small mobile and software companies, mostly startups, are most vulnerable in this case and an easy target of patent trolls.

According to the RPX Corporation (RPXC) "NPE Litigation Report," around 4,500 patent infringement lawsuits were filed in 2014. Out of those, patent trolls were responsible for 2,791 cases, i.e. 63% of the total, whereas actual operating companies filed only 1,667.

A landmark case that came as a relief for companies in the United States, as it would mitigate the threat of phoney patent suits, was decided by the United States Supreme Court recently. The Court, in ***TC Heartland v. Kraft Foods (2017),*** unanimously ruled that patent cases should be tried where the defending company is based, rather than in a court of the plaintiff's choosing. Until now, patent cases could be heard anywhere throughout the country, causing the companies to find the courts where the odds would be in their favour, often resulting in biased results and over burdening of certain courts.

However, not all the suits filed by patent troll companies are a hoax.

According to Bloomberg, Apple was ordered by a federal court in Texas to pay $502.6 million to a patent troll called VirnetX in April 2018, in an eight-year-old legal battle over FaceTime and iMessage patents. Apple and VirnetX had been fighting in court since 2010, when the patent-holding company alleged that Apple infringed on four of its patents related to internet-based communications.

Way to combat patent trolls

In order to allay the threat of patent troll litigation, companies can hire 'patent-tracking companies' on an annual-fee basis. They acquire information to track down the potentially disputable patent rights before their acquisition by patent trolls to be used against companies.

Tax Avoidance

According to Prof. Andrew Blair-Stanek of University of California, Multinational Corporations use Intellectual Property (IP) to avoid taxes on a massive scale, by transferring their IP to tax havens for artificially low prices. Read more

He states that there are two main reasons which make acquired intellectual property rights ideal for tax evasion.

- First, unlike workers or physical assets like factories or stores, IP can easily be moved to tax havens via mere paperwork.
- Second, the uniqueness of every piece of IP makes a precise fair market value nearly impossible to establish, allowing multinationals to justify low valuations that result in the least tax. Virtually all IP-based tax-avoidance schemes involve assigning an artificially low price to a piece of IP at some point in time.

Competition laws

Competition policy consists of a set of laws and regulations and policies that promotes free and fair competition in markets and aims to prevent anti-competitive business practices and unnecessary government interventions, avoiding concentration and abuse of market power. As such, competition laws and IPR may seem inherently contradictory to each other, as while Competition law prevents artificial entry barriers and seeks to remove monopolization of the production processes by encouraging entrance into industries by new players, IPR promotes the concentration of monopoly power in the hands of few.

However, when looked from a broader view, these two laws have always complemented each other in their implementation. In order to understand the complications in applying competition law and IPR simultaneously, it is important to analyse the laws adopted by several countries and how they have framed their legislation in order to counter these problems.

Harmonization of IPR and Competition Laws: TRIPS

While the negotiations over the TRIPS Agreement were going on, many countries expressed their serious concern over the regulation of unfair competition and abusive monopoly powers of the IP rights holder.

Subsequently, after much deliberations, **Article 40** of the TRIPS agreement was inserted to address the issue of IPR misuse and combat it through necessary government intervention:

Article 40

1. *Members agree that some licensing practices or conditions pertaining to intellectual property rights which restrain competition may have adverse effects on trade and may impede the transfer and dissemination of technology.*
2. *Nothing in this Agreement shall prevent Members from specifying in their legislation licensing practices or conditions that may in particular cases constitute an abuse of intellectual property rights having an adverse effect on competition in the relevant market. As provided above, a Member may adopt, consistently with the other provisions of this Agreement, appropriate measures to prevent or control such practices, which may include for example exclusive grant back conditions, conditions preventing challenges to validity and coercive package licensing, in the light of the relevant laws and regulations of that Member.*

Article 40 of the Agreement empowers the member countries to specify any exploitation of monopoly rights and adopt such laws that may be necessary to curb the abuse of IPR.

Compulsory Licensing

According to World Trade Organisation,

Compulsory licensing is when a government allows someone else to produce a patented product or process without the consent of the patent owner or plans to use the patent-protected invention itself. It is one of the flexibilities in the field of patent protection included in the WTO's agreement on intellectual property — the TRIPS (Trade-Related Aspects of Intellectual Property Rights) Agreement.

The right over the product still rests with the owner, who is entitled to royalty by the users. This is an effective statutory measure to deter complete control of the owner over the unfettered use (or misuse) of the product.

Article 31 of the TRIPS agreement provides for the grant of compulsory licensing under certain exceptional situations such as national emergency or other circumstances of extreme urgency or inadequate exploitation of the patent in the country.

Conclusion

Intellectual Property Rights have so far proved to be a boon for mankind by promoting inventions and rewarding intellect, thereby spurring economic growth and by creating new jobs and industries. According to WIPO:

An efficient and equitable intellectual property system can help all countries to realize intellectual property's potential as a catalyst for economic development and social and cultural well-being. The intellectual property system helps strike a balance between the interests of innovators and the public interest, providing an environment in which creativity and invention can flourish, for the benefit of all.

However, abuse of such rights may undermine the spirit and defeat the purpose of granting them. Their misuse yields nothing but increased costs, mental stress, tainted reputation and depleted growth of businesses.