Living in the 21st century, it is impossible to imagine a day without the internet. With the ever-growing advancement in the field of technology, the world is at our fingertips. One-click and we can access anything and everything within a fraction of a second. From chatting to calling, buying and selling, shopping or making payments, from business to entertainment, and now with the world at a standstill; adapting to the concept of work from home, there is nothing a person can't achieve with the internet.

But with every good thing that the internet has to provide there are also a few drawbacks to it. This is where the term cybercrime comes into place.

Cybercrime in simpler words is linked to the idea of criminal activities that take place through a computer network or by hacking a computer network. Such activity is carried out to earn profit or corrupt information available online, to gain access to an individual’s private or corporate data, to defame a person, or to cause fraud. Cybercriminals can also attack an entire computer network by infecting a single computer with malware or virus which then spreads to the entire computer network.

Cybercrimes can be broadly categorized into three types:

1. Crime against the person - in this type of cybercrime the victim is usually a person. The objective of cybercrime against a person is to ruin his image by sending defamatory emails or messages on social media networks.

   Cybercriminals can hack the computer network of an individual to extract sensitive information or gain unauthorized access which can then be used against them as blackmail or to gain unauthorized access to the person’s bank account to steal money.

   At times social media accounts of people are hacked and used to post or delete content which would ruin the reputation of people.

   Hosting a website that contains prohibited images or videos such as pornography can also lead to cybercrime as it can cause harm to the mind of the young generation. Creating or accessing or distributing of such content is also considered to be a part of cybercrime and is prohibited especially in the case of child pornography.

   Cyberstalking is another form of cybercrime against a person. Here the person, or the family members are threatened through texts, calls emails or videos.

2. Crimes against property - in this type of cybercrime the main objective of cybercriminals is to obtain money or confidential information through fraud or unauthorized access.

   With the increasing growth in the occupational sector, the day-to-day working of people depends on the internet. From making transactions to keeping check of the stock of goods available and also the documents regarding the firm or company;
all of this information can be stored and also managed through a single computer device.

But all this information regarding the company’s trade secrets or important contracts or any such information stored in the computer gives a motive to the cybercriminals who find unauthorized access to these files to exploit the people or the firm at large or to use the trade secrets for their benefit.

The other reason behind such activities is gaining reputation and profit by creating a brand or website with the name or logo similar to that of a well-known company which fools commoners to fall into the trap and use the new similar brand believing to have the goodwill same as the original. These kinds of tricks are used to gain benefits from intellectual properties and exploit the rights and benefits owned by these well-known brands or companies.

Also, hackers access the social media accounts of such companies to post content that would diminish their reputation which in certain cases also leads to financial losses to these companies.

3. Crime against the government- in this type of cybercrime the government bodies are threatened to give away confidential information or into deleting certain information for the benefit of the cybercriminals.

Through sedition, people can be enticed or also be forced into rebelling against the government which in certain cases leads to an increase in terrorist activities. Cybercriminals can hack into government records to steal military secrets that they can use it while planning any terrorist activities or spy on the day-to-day activities of the government.

**Working of cybercrime:**

Any kind of criminal activity required a motive and that’s exactly what a cybercriminal does. Having the motive to hack into a person’s database to steal unauthorized information, or defame a person, or fraudulently take away someone else’s money or destroy any kind of information available online, or threaten to cause harm to the person or family. No matter what type of cybercrime takes place, it always causes harm to person be it physical or financial.

Cybercrime can be carried out from anywhere around the world. The only requirement is a computer or computer system with an internet facility. Such activities can be carried by a single person who just wants to harm a particular person due to just personal grudges or by an entire team or cybercriminals who are hired by other people or various agencies to attack a large number of people, small firm to multinational companies or even government authorities.

To carry out any kind of cyber activity required various software that is available online through the dark web. It is through the dark web where many kinds of illegal activity take place. No one can access the content available on the dark web without proper means. It is only through authorization and the use of particular browsers can a person use the dark web. It is mostly used by hackers or cyberbullies to purchase illegal software which they then use to carry out cybercrime.

This means that cybercrime requires a medium. Between the cybercriminal and the person being attacked, there is a source that connects them. This source is made available...
through a third party and this third party can be approached through the dark web who providing the cybercriminal with the software or a malware code which can then be used to disrupt the files of the person under attack.

Cybercriminals also use the dark web to create accounts using cryptocurrency where they can keep the money safe which they acquire from people online or by calling people seeking one-time password (OTP) to carry out transactions consisting of a large amount of money. Once these transactions take place and the money is transferred to accounts using the dark web it cannot be traced back to the cybercriminal and hence there is no way possible to recover the money. The dark web is a wide concept. And as most of these activities are untraceable, there is no easy way to catch these cybercriminals or to even prevent these activities from happening.

**Personal Measure:**

As a regular user of computer networks and internet facilities, there is always a threat to our data. And with the ever-increasing cases of cybercrime there is a constant need to maintain a comprehensive cyber security policy.

The first major step to remember when any kind of cybercrime activity takes place is to report it to the nearest police station or the cybercrime branch or the cyber cell. In case an unauthorized transaction takes place, it is important to inform the bank as soon as possible so that the transaction can be stopped. Recovery of stolen money or any other information is only possible if such crime is reported. Only then can the concerned authorities take the necessary action and help the victim.

The easiest and yet very important measure to follow is keeping a password that’s not easy to crack. The easier the password; the easier it is to hack into someone’s data, be it a computer or any of the social media platforms or mail. And once the hacker cracks the password, everything available on the system or the internet becomes accessible to the cybercriminal who can then easily disrupt the data.

Another way to ensure security is keeping a computer or mobile devices, applications, and software updated all the time, as it is easier to attack a system with malware or virus. Updating a system repairs bugs or flaws in the system and hence keeping a check on the available software updates or keeping auto-updates on is a way to protect devices from being malware-infected.

Data on the internet is easily accessible to anyone and everyone and so it is important to remember to keep the personal information secured and to keep a check on who has the access to the data while posting anything on social media. It is suggested to keep the social media account private to prevent unwanted people from getting access to personal data.

Malware attacks can also lead to data disruption as a result of which important data stored in the computer system can be lost. And so, to prevent this; regular backup should be made in case any data is lost as it can be recovered.

Fraud calls seeking one time password (OTP) or sometimes even ATM pins is something a person should be aware of. Cybercriminals pretend to be associated with big companies selling policies or goods and ask for personal information which can be used to withdraw money from the person’s account. Once the
money is transferred there is no way to trace the money or even recover it.

Even after constant messages being forwarded by banks or government or even on social media platforms to not share the personal details with anyone, people still fall for traps believing to achieve huge monetary advancement from these fraud calls but instead end up with an empty bank balance.

Sometimes these fraud messages can also be forwarded via messages or mail or social media platforms like WhatsApp, Instagram, or Facebook. It is important to verify the source of such messages before accepting any of its terms. Over the years, social media has become a huge influence on people but also a platform for cybercriminals to carry out fraud and so being cautious with what information to believe in and what not to is necessary.

Information Technology Act, 2000-

In the year 2000, the Information Technology Act came into force to prevent the increasing cases relating to computers and computer networks located in India. This act came into force on the 17th of October 2000, and it applies to the whole of India.

In India, there is no particular Act relating to cybercrime but there are a few sections relating to cybercrime in the Information Technology Act, 2020. It is because of this act that activities such as hacking, identity theft, spreading of the viruses, circulation of pirated movies or songs, pornography or child pornography, sending defamatory messages or emails, data theft, or terrorism were made criminal offenses.

The Information Technology Act, 2000 also prescribes a set of rules for the functioning of cyber cafes, website blocking, data security, and electronic service delivery.

**Important sections of IT Act 2000:**

Section 3: It deals with the authentication of electronic records which are done by the asymmetric cryptosystem and by transforming electronic records into another.

Section 4: This section is about the legal recognition of electronic records. It means that information or any other documents in writing or the printed form shall be deemed to be made available in an electronic form.

Section 6: This section is about electronic governance. According to this section, the use of electronic records and digital signatures in Government and its agencies is made authentic.

Section 17: This section gives a plan of action for regulation of appointment of controller and deputy controller of certifying authorities and other officials under the Central Government.

Section 18: This section talks about the functions of the controller of certifying authorities such as;

A) laying down the standard

B) maintaining a database

C) and the form and manner in which account shall be maintained by the controller

Section 35-39: These sections of the act deal with the thing related to the digital signature certificate such as revocation and suspension of the digital signature certificate.
Section 41: This section deals with the duties and responsibilities of subscribers. The subscriber shall be liable until he has informed the certifying authority that the private key has been compromised.

Section 43: This section is about penalties, compensation, and adjudication for damages to Computer, Computer systems, unauthorized access, download of data, infecting with virus, denial of access, etc.

Section 44: This section talks about the penalty for failure to furnish information, returns, etc. to the certifying authority.

Section 48: This section is about the establishment of a Cyber appellate tribunal. The cyber appellate tribunal shall exercise the jurisdiction, power, and authority conferred to it under this Act.

Section 55: This section deals with the formation authenticity of the appellate tribunal. Orders constituting appellate tribunal to be final and not to invalidate its proceedings before an appellate tribunal.

Section 60: This section of the Act talks about the limitation of the tribunal. The provision of the limitation Act 1963 shall apply to the appellate tribunal.

Section 65: This section is about the penalty for tampering with computer source documents. Whoever knowingly or intentionally destroy, conceal or alter any computer source code, shall be punished with imprisonment up to three years.

Section 66: This section of the Act is about the penalties for computer-related offenses. The punishment for the hacking of computer is up to three years or with a fine which may extend to five lakh rupees.

Section 66B: This deals with the penalty for dishonestly receiving stolen computers or communication devices.

Section 66C: This section deals with the penalty for identity theft which may extend up to three years.

Section 66D: This section is about the punishment for cheating by personation by using computer resources.

Section 66E: This section deals with the penalty for capturing, transmit of publishable images of a person without consent regardless of whether that person is in a public or private place.

Section 66F: This section is about the penalties for cyber terrorism like

A) denying access to any other person authorized to access computer resources
B) introducing any computer contaminant.

Section 67: This section deals with the punishment for publishing information that is obscene in electronic form which may extend up to three years of imprisonment.

Section 67A: This section of the Act deals with the penalty for publishing images containing sexual acts or conduct.

Section 67B: This section deals with the penalty for publishing or transmitting material illustrating children in sexually explicit content.

Section 70: This section is about the penalties for securing access or attempting to secure access to a protected system. The government may declare any computer which affects the facility of criminal information infrastructure, to be a protected system.
Section 71: This deals with the penalty for misrepresentation to or suppresses any material fact.

**Conclusion:**

Cybercrime is an evolving concept. With the constant development in the field of technology, the internet has become essential to the day-to-day functioning of a human being. But with every good improvement, there is a reason to worry about. It is a crime by the human against humans. To completely eradicate cybercrime is not easy but with the help of law, cyber cell, and also with some precautions on a personal level it’s a war worth fighting for.