CYBER CRIME

Introduction

The most discussed subject of the twenty-first century is cybercrime. The usage of cellphones and the internet is increasing dramatically over the world, which is generating questions about consumers' security and privacy.

Computer related networks that involve the use of computers, networks and gadgets can be interconnected to a cybercrime. In such crimes, the security of networks, persons, institutions or a whole nation could be at risk and threat. Hackers steal confidential data in unethical ways and utilize this information and data for spurious purposes. Cybercrimes are high functional frauds that can wipe off big online financial transactions and transfer the entire amount into criminal accounts.

Cyber Crime-

The systematic illegal behaviour carried out digitally and carried out by attackers is referred to as cybercrime or attack. There are numerous instances of cybercrime, such as fraud, viruses and malware, cyberstalking, and others.

Due to these, businesses and government organizations are spending more on maintaining and employing professionals in cybercrime. Cybercrime was formerly only committed by lone individuals or small groups. However, a sophisticated network of cybercriminals is currently working to attack the system for data collecting.

Cybercrimes may include credit card frauds, voice phishing, distribution of viruses, cyber-stalking, child pornography, forgery, unauthorized access, etc. This is a fast-growing area of crime that happens over the internet. With the advancement in technology, we are leaning towards the internet all the more. It is needed for numerous activities like social networking, gaming, transaction, e-commerce, online studies, shopping, job seeking, etc.

The first case was recorded in 1820. It has been said that in these recent few years, at least 4000 cases have been filed in Malaysia. All of these cases consist of fraud, malware; file loss, hack threats, and denial of services. Major crime areas as per the government include piracy, cracking,

and cyber-terrorism. Since more and more people are using computers, these types of cyber crimes will only keep increasing.

India and many other nations are dealing with the same crisis. An article reported China in itself has near about 300 million internet users. Criminals rely on computers as it is networked internationally. These criminals are organized and individual hackers. They mostly get involved for two reasons. The first one is that they want to prove themselves to be excellent at breaching computer software. The second reason is for monetary purposes. They mostly target big companies, organizations, or banks.

The rate of data circulation has increased as a result of the internet's improved speed. To protect all the organizations, it is crucial to take action against these illegal acts through investigation, control, and prevention. Our government must acquire highly qualified cybercrime knowledge. This will assist in regulating this serious problem.

Types of Cyber Crimes

There is a range of activities that fall into the category of cyber crime. Let us take a look at them.

- **Hacking:** It refers to breaking into a person's computer system without his/her knowledge or consent. It is also known as unauthorized trespassing in the cyber world. Hackers can access sensitive information of the user (like identity details, passwords, and credit card information).
- **Cyber Stalking:** This is one of the worst ways to harass a person. Victims of cyber-stalking are subjected to tons of messages and emails by the stalkers. Not responding to these often leads to grave outcomes.
- **Identity Theft:** Here, the person's identity gets stolen. This includes his/her name, bank details, social security number, birthday, credit or debit cards, etc. This information is misused by the criminals to commit fraudulent activities (like applying for new credit cards, getting medical services, collecting loans) which hamper the owner's record.
- **Phishing:** This is a kind of email fraud wherein various mails are sent to the people. The content of the mail mostly seeks financial information of the person. These emails might look like they are coming from an authentic source (but they are not).
- **Malware:** It is Internet-based software that is programmed to damage a computer system.
- **Computer vandalism:** This type of cyber crime destroys a computer's data by transmitting viruses.

- **Theft:** It occurs when a person violates copyrights regulation. This is mostly noticed while downloading music, movies, or even games.
- **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.

Laws related to Cyber Crimes

In order to combat cybercrimes, the government has created a number of strict regulations. These regulations will serve to protect our interests. Additionally, they will help in reducing these crimes. The police stations now have cyber units that can monitor the issue immediately. In India, there are often three categories used to classify cybercrimes. These are the Indian Penal Code, the IT Act, and the State Legislation. Section 66E and 67B of Information Technology Act, 2000are related to MMS forwarding and Child pornography respectively.

The Ministry of Home Affairs has advised the State government to include facilities like technical infrastructure and skilled manpower to curb the cases of cyber crimes. Cyber Crime Police Officers can now receive training at the Forensic Lab of CBI.

Kerala, Tripura, Assam, and many other Indian states have started the training procedures. The Ministry of Home Affairs has also come up with an open platform (I4C) to fight against these crimes. I4C (Indian Cyber Crime Coordination Centre) helps victims to raise their complaints.

How to Prevent Cyber Crime

We must take action to stop these crimes now that we have these cyberlaws in place. If we wish to protect ourselves, we must adopt protective precautions. We must first be conscious of our internet transactions. If we have spyware on our computer, we could lose crucial information (and we are unaware of it).

Installing updated antivirus software is crucial. In addition, only 50% of the populace is even aware of these crimes. They need to be taught how to use computers, the internet, credit cards, etc. Furthermore, they ought to be aware of the government's initiatives. Being vigilant is also the greatest method to combat this issue.

Conclusion

Technology development has led to the emergence of unpleasant aspects on the dark web. Intelligent people have turned the Internet into a tool for wicked activities, which they occasionally use for financial benefit. Cyber laws therefore enter the picture at this time and are crucial for every person. Some actions are categorized as grey activities that are not subject to legal regulation since cyberspace is a very challenging environment to deal with.

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.