Shodhshauryam, International Scientific Refereed Research Journal
© 2023 SHISRRJ | Volume 6 | Issue 1 | ISSN : 2581- 6306

Cyber Crime : Types, Pattern & Prospects

Dr. Raghuvir Singh
Assistant Professor, G. S. Law College Auraiya, U.P., India

Article Info

Publication Issue :
January-February-2023
Volume 6, Issue 1

Page Number : 154-167

Article History
Received : 01 Jan 2023
Published : 20 Jan 2023

ABSTRACT- As fast as we are moving towards the digital world, the number of cyber crimes is also increasing at the same rate. The pace at which technology has progressed; at the same pace man's dependence on the internet has also increased. By sitting at one place, through the Internet, man's access has become easy to every corner of the world.In today's time, everything that a person can think of can be accessed through the internet, such as social networking, online shopping, storing data, gaming, online study, online job etc. In today's time, internet is used in almost every field. With the growth of the Internet and its associated benefits, the concept of cyber crimes has also evolved.Currently, a large population of India uses social networking sites. There is a lack of awareness among people regarding the use of social networking sites in India. Also, most of the social networking sites have their servers abroad, which makes it difficult to reach the root cause of cyber crime in India.Cyber crimes are essentially criminal activities where a computer, network or electronic information technology device is the source, instrument, target or location of the crime. Cyber crimes occur through illegal access to other data bases, illegal interception, data interference, system interference, misuse of equipment, forgery and electronic scam. In this article cyber crime, its types, preventive measures and provisions made by the government have been discussed. Along with this, the role of social networking sites in cyber crime was also evaluated.

Keywords - CyberCrime, Cyber Security, Internet, Hacking, Awareness.

INTRODUCTION- Cyber crimes are committed in various forms. A few years back, there was a lack of awareness about the crimes committed through the internet. In the matter of cyber crimes, India is also not far behind those countries, where the rate of incidents of cyber crimes is also increasing day by day. In cases of cyber crime, a cyber criminal can use a device to gain access to a user's personal information, confidential business information and government information or to disable a device. Selling or buying information online is also a cyber crime.

It is a medium which is infinite and immeasurable. Whatsoever the good internet does to us, it has its dark sides too.[1] Cybercrime that has a significant financial impact includes ransomware attacks, email and Internet

[1] Prof. R.K.Chaubey, "An Introduction to Cyber Crime and Cyber law", Kamal Law House, 2012

Copyright: © the author(s), publisher and licensee Technoscience Academy. This is an open-access article distributed under the terms of the Creative Commons Attribution Non-Commercial License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited

fraud, identity fraud, and attempts to steal financial account, credit card, or other payment card information that are committed using computers and the Internet. Is. Cyber crime, also known as 'electronic crime', is a crime in which a computer, network device or network is used as an object or tool to commit a crime.

Such crimes include a wide range of activities, including cyber extortion, identity theft, credit card fraud, hacking personal data from computers, phishing, illegal downloading, cyber stalking virus spreading, among others. It is worth mentioning that software piracy is also a form of cyber crime, in which it is not necessary that cyber criminals commit crime through online portal only. In India, cyber crimes are covered by the Indian Penal Code of 1860 and the Information Technology Act of 2000. Issues relating to cybercrime and electronic commerce are dealt with in the Information Technology Act 2000, which was amended in 2008 to outline the definition and punishment for cybercrime. The IT Act of 2000 in India addresses the issues of cybercrime. "against persons or groups of persons with the criminal intent of intentionally harming the reputation of the victim or causing physical or mental harm or harm directly or indirectly to the victim using modern telecommunication networks (networks including chat rooms) such as the Internet crimes committed, email, notice boards, and groups) and mobile phones"

Hence cyber crime can be described as a mixture of technology and crime. Simply put, "any act or crime that involves the use of a computer" is a cyber crime. Consequently, "CyberCrime" can be described as any crime that is committed using an electronic communication or information system, such as any device or the Internet, or both or both.

HISTORY AND ORIGIN OF CYBER CRIME- In the early 1970s, criminals regularly committed crimes through telephone lines. The criminals were called eccentrics. In fact, there was no real cybercrime until the 1980s. A person had access to another person's computer in order to search, copy, or manipulate personal data and information. *The first person to be convicted of cybercrime was Lan Murphy, also known as Captain Zap, and this happened in 1981*. They hacked the US telephone company to manipulate it's internal clock so that users could still make free calls during peak hours times.[2]

CLASSIFICATION or PATTERN OF THE CYBER CRIME -According to cyber experts, the category of cyber crime can be divided into three categories- Crimes in which computers are attacked. Examples of such crimes are hacking, virus attacks, etc. Crimes in which computer is used as a weapon/tool/. These types of crimes include cyber terrorism, IPR infringement, credit card fraud, pornography etc.[3] Cyber crime is broadly categories into three areas –

Personal: It is a cyber crime in which a person disseminates malicious or illegal material through the Internet. For example, distribution of pornography, human trafficking and online stalking.

Assets: This cybercrime involves gaining access to individuals' bank or credit card information, accessing their funds, conducting online transactions, or executing phishing schemes to persuade individuals to give up personal information.

Government: While these cybercrimes are uncommon, they are still considered significant crimes. This includes breaking into government databases and hacking official websites.

[2] https://goosevpn.com/blog/origin-cybercrime
[3] https://www.swierlaw.com/faqs/what-are-the-three-types-of-cyber-crimes-.cfm

DIFFERENT TYPES OF CYBER CRIME- In this time many types of cyber crimes the most common are e-mail fraud, social media fraud, banking fraud, ransomware attacks, cyber espionage, identity theft, clickjacking, spyware etc.[4] According to the classification, the different types of cyber crimes are following –

Cyber Crime Against Persons- Cyber crimes committed against persons include various crimes like transmission of childpornography, harassment of any one with the use of a computer such as e-mail. The trafficking, distribution, posting, and dissemination of obscene material including pornography and indecent exposure, constitutes one of the most important Cyber crimes known today.[5] Offenses which affect persons which are as follows -

1. **Cyber-stalking:** It means creating a physical threat that creates fear using computer technology such as the Internet, e-mail, phone, text message, webcam, website, or video.
2. **Proliferation of obscene material:** This includes indecent exposure/pornography (basically child pornography), hosting a web site containing these prohibited materials. These obscene matters can harm the mind of the teenagers and corrupt or corrupt their mind.
3. **Defamation**: It is an act of alleging to lower the dignity of a person by hacking his mail account and sending some mails using obscene language in the mail account of unknown persons.
4. **Hacking**: It means unauthorized control/access to the computer system and the act of hacking completely destroys the entire data as well as computer programs. Usually hackers hack into telecommunication and mobile networks.
5. **Cracking**: This is one of the serious cyber crimes known so far. Cracking means that a stranger has broken into your computer system without your knowledge and consent and tampered with the valuable confidential data and information.
6. **Email Spoofing:** Forged e-mail can be said to be one that misrepresents its origin. It refers to its origin as being different from that from which it actually originates.
7. **SMS Spoofing:** Spoofing is a blocking through spam which means unwanted uninvited messages. The wrongdoer steals the mobile phone number of any person and sends SMS through internet and the recipient gets the SMS from the victim's mobile phone number. This is a very serious cyber crime against any individual.
8. **Carding:** It refers to fake ATM cards i.e. debit and credit cards, which are used by criminals for their monetary gains by way of maliciously withdrawing money from the victim's bank account. These types of cyber crimes always involve unauthorized use of ATM cards.
9. **Cheating and Fraud**: It means that the person who is committing the act of cybercrime i.e. stealing password and data storage has done so with a guilty mind which causes fraud and cheating.
10. **Child Pornography**: This involves the use of a computer network to create, distribute, or access material that sexually exploits children under age.

[4] https://intellipaat.com/blog/what-is-cybercrime/
[5] http://ijiet.com/wp-content/uploads/2013/07/32.pdf

11 **Threatened Assault:** Threatening to put a person in fear for his life or the life of his family through a computer network i.e. e-mail, video or phone.

Crimes Against Property - Since there has been a rapid increase in international trade where businesses and consumers are using computers to create, transmit and store information in electronic form instead of traditional paper documents. Offenses which affect the properties of persons which are as follows –

- **Intellectual Property Offenses**: A copyright is the legal right of an author, publisher, composer, or other person who creates a work to exclusively print, publish, distribute, or perform the work in public.[6] Intellectual property consists of a bundle of rights. Any illegal act by which the owner is fully or partially deprived of his rights is an offence. The common form of IPR infringement can be termed as software piracy, infringement of copyright, trademark, patent, design and service mark infringement, theft of computer source code, etc.
- **Cyber squatting**: This means where two persons lay claim to the same domain name either by claiming that they had registered the first name with the right to use it before the other or by using something similar to the first. For example two similar names i.e. www.google.com and www.google.com.
- **Hacking Computer Systems**: Hacktivism attacks computers by unauthorized access/control over them including the famous Twitter, blogging platform. There will be loss of data as well as computer due to hacking activity. At the same time, research specifically indicates that the purpose of those attacks was not even primarily financial gain, but to lower the reputation of a particular person or company.
- **Cyber Vandalism**: Vandalism means intentionally destroying or damaging the property of another. Thus cyber vandalism means destruction or damage of data when a network service is down or disrupted. Its scope may include physical damage of any kind to any person's computer. These acts may take the form of theft of the computer, computer parts, or other equipment connected to the computer.
- **Transmitting Virus:** Viruses are programs that attach themselves to a computer or file and then transmit themselves to other files and to other computers on the network. They usually affect the data present on the computer by either changing or deleting it. Worm attacks play a major role in affecting the computerized system of the individuals.
- **Cyber Trespassing**: It means accessing someone's computer without proper authorization of the owner and does not disturb, alter, misuse or damage the data or system by using wireless internet connection.
- **Internet Time Theft:** Basically internet time theft comes under hacking. This is the use by an unauthorized person of Internet hours paid for by another person. A person who obtains someone else's ISP user ID and password by hacking or gaining access illegally, uses it to access the Internet without the other person's knowledge. You can identify time theft if your internet time has to be recharged frequently despite frequent use.

[6] Cyber Ctimes and Laws, Dr. U.S. Pandey, Dr. V. Kumar, Dr. H.P. Himalya Publshing House- 2017 p-15

Cyber Crimes Against The Government - This is considered the most serious cyber crime. Such crime committed against the government is also known as cyber terrorism. Government cyber crime includes hacking of government website or military website.[7] Significantly, when a cybercrime is committed against a government, it is considered an attack on the sovereignty of that nation and an act of war. These perpetrators are usually terrorists or governments of other hostile countries. Strict cyber laws have been made by the government of every country to control such cyber crimes. Crimes that affect the government are as follows –

- **Cyber terrorism:** Cyber terrorism is a major burning issue of domestic as well as global concern. Common forms of these terrorist attacks on the Internet are distributed denial of service attacks, hate websites and hate e-mails, attacks on sensitive computer networks, etc. The activities of cyber terrorism threaten the sovereignty and integrity of the nation.
- **Cyber warfare**: This refers to politically motivated hacking to cause harm and espionage. It is a form of information warfare that is sometimes seen as analogous to conventional warfare, although this analogy is controversial for both its accuracy and political motivation.
- **Distribution of Pirated** Software: It means to distribute pirated software from one computer to another with the intention of destroying the data and official records of the Government.
- **Possession of Unauthorized Information**: With the help of internet it is very easy for terrorists to access any information and keep that information with them for political, religious, social, ideological purposes.

ROLE OF SOCIAL MEDIA - The population using social networking sites on a large scale is unaware of the dangers of cybercrime. The servers of various social networking sites are concentrated in other countries, leading to fears that these countries may misuse people's personal information.People share their personal information on various social networking sites, due to which hackers easily hack these social networking accounts and then misuse the information received.Hackers on social networking sites make people victims of online fraud.It has also been detected by security agencies that funding of terrorists and anti-national elements is done through various online money transfer apps. Cyber criminals encourage children to commit crimes through various online games.

IMPACT OF CYBER CRIME – Cyber crime can take many forms, be it online scams for petty theft or more serious threats like terrorism. Whatever the case, its effects can be incredibly damaging to society. A cyberattack can have tremendous negative psychological effects, with the effects felt by victims for weeks or even months.

[7] https://www.legalserviceindia.com/legal/article-2436-cyber-crime-and-terrorism.html

Impact of Cyber Crimes on Trades- Assume that an e-commerce trades collects card details of customers when a customer makes an online payment. This huge corporation has millions of customers. Now say, at least 70% of their customers pay using debit cards, credit cards, UPI, digital wallets etc. This means that the business has built up a huge online customer database. If a company does not take adequate measures to secure and encrypt the sensitive financial information of its customers, hackers can exploit even the smallest of vulnerabilities and hack into internal systems. They can access customers' card information and track it back to their bank accounts and steal money. This can cause economic loss to many people, which can cause huge upheaval in the society.

Impact of CyberCrimes on Infrastructure - Cyber terrorism is also a significant threat to the society. Cyber terrorists can break into systems that control infrastructure such as air traffic control and put millions of lives at risk. The more technologically advanced a nation is, the greater the risk of cyber terrorism.

Cybercriminals can also target healthcare websites. They can expose sensitive data of patients and hospital staff. In recent days, there was information about cyber attack on All India Institute of Medical Sciences (AIIMS) through media.

These cyber crimes can range from malware and denial-of-service. Cyber attacks on the healthcare industry can have effects that go beyond financial loss, meaning they can pose a risk to patients' lives.

Impact of Cyber Crime on Individuals- Cyberbullying involves blackmailing Internet users by threatening to leak false information. Like attacks on healthcare, the consequences of cybercrime are not limited to financial loss. Victims may suffer from conditions such as anxiety and depression, leading to suicidal tendencies.

Thanks to digitization, but our phones aren't the only possessions that have become smart. Rather, Artificial Intelligence (AI) and the Internet of Things (IoT) have enabled smart homes, where you can turn on any device with a voice command. Your new-age Smart TV allows you to subscribe to various streaming platforms, but the absence of a legitimate security system leaves your payment details.

MOST FAMOUS CYBER ATTACKS ON HISTORY- Cyber attacks are on the rise. While modern technology presents many conveniences and benefits, there are people who misuse it which poses a threat to businesses and data privacy globally.

When a data breach occurs, it can have far-reaching effects. It goes beyond the target company, affecting customers, suppliers and others. Amazingly, experts expect the cost of cybercrime to reach around $10.5 trillion by 2025.[8] Humans always learn from the past Historical cyber attacks that can be learned from-

1. Melissa virus- One of the earliest and biggest cyber threats came from the Melissa virus in 1999 by programmer David Lee Smith. He sent users a file to open through Microsoft Word, which contained the virus. Once opened, the virus becomes active, causing serious damage to hundreds of companies, including Microsoft. It is estimated that $80 million will be spent to repair the affected systems.

2. NASA Cyber Attack- In 1999, 15-year-old James Jonathan hacked into NASA's computers and shut them down for 21 days! About 1.7 million software downloads were downloaded during the attack, which cost about $41,000 to repair.

[8] https://clearinsurance.com.au/10-biggest-cyber-attacks-in-history/

3. 2007 Estonia cyber attack- In April 2007, Estonia saw the first cyber attack on an entire county. Notably, it saw around 58 Estonian websites go offline, including government, bank and media websites.

4. Cyber attack on Sony's PlayStation Network- In April 2011, a cyber attack on Sony's PlayStation Network compromised the personal information of 77 million users.

5. Adobe Cyber Attack- The Adobe cyberattack was previously thought to have breached the data of 2.9 million users. Furthermore, it compromised the personal data of 38 million users! Adobe claims that only the passwords and credit card information of the first 2.9 million users were compromised, however, the remaining 35.1 million suffered the loss of their passwords and user IDs.

6. 2014 Cyber Attack on Yahoo- In 2014, Yahoo was the site of one of the biggest cyber attacks of the year when 500 million accounts were compromised. During the attack, basic information and passwords were stolen, while bank information was not.

7. Ukraine's Power Grid Attack- Ukraine's power grid attack in 2015 was the first cyber attack on the power grid. As a result of the attack, about half of the homes in the Ivano-Frankivsk region of Ukraine were without electricity for a few hours.

8. 2017 WannaCry Ransomware Cyber Attack- One of the largest ransomware attacks ever occurred in 2017. Furthermore, it affected approximately 200,000 computers in over 150 countries. In short, the ransomware had a huge impact on many industries, costing the global approximately £6 billion to fix!

9. Cyber attack on Marriott Hotels- A cyber attack on Marriott Hotels and Starwood Hotel Group didn't happen for years, only to come to light in 2018. Thus, by the time they became aware of the attack, an estimated 339 million guests' data had been compromised. As a result, the UK's data privacy watchdog fined Marriott Hotels £18.4 million.

10. Biggest password leak ever- In June 2021, we saw a compilation of approximately 8.4 billion passwords leaked in the RockYou2021 attack. In fact, it was the biggest breach since the RockYou site in 2009 that affected 32 million accounts.

While technology and data protection tools are evolving, so are cyber criminals to trick businesses and employees into clicking on links and documents within emails. Therefore, to help businesses prepare, our blog on 10 steps to protect your business from cybercrime highlights easy ways to protect your business from cybercrime.

INTERNATIONAL REFELACTION ON CYBER CRIME- The need for international cooperation to promote cybercrime and data security is being emphasized by the Ministry of Home Affairs for signing the Budapest Convention on cybercrime. The Budapest Convention on Cybercrime is a convention known as the Budapest Convention on Cybercrime. It is the first international treaty of its kind which sought to curb internet and computer crimes by streamlining national laws, improving investigative techniques and increasing cooperation among other countries of the world in this regard.

Article 32B of the Convention allows access to data and thus violates national sovereignty, so Brazil and India have refused to sign the Convention as they were not involved in its formulation. Russia has opposed the convention on the grounds that it would violate Russian sovereignty if adopted.

The Budapest convention - The Council of Europe Convention on Cybercrime ('the Convention') was the first multilateral binding instrument to regulate cybercrime.[9] Having recently passed the 20th anniversary of its entry into force, the convention's role is now in line with several international, regional and national initiatives in harmonizing cybercrime laws and other international efforts to combat cybercrime. In an environment where an international agreement may be some distance away, the Convention provides an important touchstone against which national efforts can be measured. More broadly, international attention is shifting in the right way to the more pressing issue of capacity building.

The Octopus Conference - Octopus Conference, organized every 12 to 18 months by the Council of Europe, is one of the largest and best platforms for exchange in cybercrime gathering experts from 80 countries, international organizations, the private sector and academia. Each Octopus conference has a specific focus related to the latest cybercrime issue.

CyberSouth – CyberSouth is a joint project of the European Union (European Neighborhood Instrument) and the Council of Europe. CyberSouth aims to strengthen legislation and institutional capacities on cybercrime and electronic evidence in the Southern Neighborhood region in line with the requirements of human rights and legislation.

CyberEast – Cyber East is a joint project of the European Union and the Council of Europe implemented in the Eastern Partnership (EAP) region by the Council of Europe under the European Neighborhood East Instrument (ENI).

Participating countries: Moldova, Armenia, Belarus, Georgia, Azerbaijan and Ukraine.

The objective of the project is to adopt a legislative and policy framework in line with the Budapest Convention on Cybercrime and related instruments, strengthen the capacities of judicial and law enforcement authorities and inter-agency cooperation, and efficient international cooperation and cooperation in criminal justice, cybercrime and electronic evidence. To increase trust, including between service providers and law enforcement.

CYBER SECURITY- The term Cyber Security refers to security on the Internet, that is, when you use the Internet, your important data, devices, software, networks, and your identity are at risk of being stolen, misused, or hacked on the Internet. .

In today's time, every work is being done on the Internet, whether it is the work of a government or private company or the personal data of a mobile Internet user, that is, every type of data is exchanged on the Internet in some form or the other. Happening.

Users' devices such as computers, servers, laptops, mobile phones or all other types of smart devices are also connected to the Internet, due to which the threat to the security of data is also increasing.

Kinds of Cyber Security- There are many different layers of cyber security, through which both hardware devices and software are used to provide maximum protection to a network or an Internet user.

Network & Gateway Security: - This can be called the first layer of the network, by which the incoming and outgoing traffic of the network is controlled, and Threats and Attacks coming into the network are prevented. Firewall Device is mainly used in this.

[9] https://www.coe.int/en/web/cybercrime/the-budapest-convention

Application Security: - The development and installation phase of all the applications used in the network are kept in mind, so that there is no shortage in them. If an application is also to be installed in the network, then a security process is passed, in which password is mandatory for its installation and Limited User Rights are imposed.

Network Access Control (NAC): - There is a very secure process to connect to the network, in which policies are made according to the users and their network rights are limited.

Data Loss Prevention (DLP): - The security of data is increased by this process, in which there is no risk of data theft or leaking, that is, the data is completely encoded.

Email Security: - Email security devices such as Spam Filters hardware or software are used to prevent threats from email.

Antivirus & Anti Spyware Software :- The most important security in network security is that of the computer, for which it is very important to have antivirus software in the computer, so that the damage caused by the virus can be prevented.

Along with all these security layers, an Internet user is also required to follow some rules at his level, such as using strong passwords and not opening unknown email attachments.

CYBER LAWS- In today's tech-savvy environment, the world is becoming more and more digitally sophisticated and so are crimes. The Internet was initially developed as a research and information sharing tool and in an unregulated manner. As time passed it started dealing more with e-business, e-commerce, e-governance and e-procurement etc. All legal issues related to internet crime are dealt with through cyber laws. As the number of internet users is increasing, the need for cyber laws and their application has also increased significantly. In today's highly digitized world, almost everyone is affected by cyber law.

Cyber crime cases like online banking fraud, online share trading fraud, source code theft, credit card fraud, tax evasion, virus attacks, cyber sabotage, phishing attacks, email hijacking, denial of service, hacking, obscenity etc. are becoming common. Digital signatures and e-contracts are fast replacing the traditional way of doing business.

Importance Of Cyber Laws- We are living in a highly digitized world. All companies depend on their computer networks and keep their valuable data in electronic form. Government forms including income tax returns, company law forms etc. are now filled in electronic form. Consumers are increasingly using credit cards for purchases. Most of the people are using email, cell phone and SMS messages for communication. Even in "non-cyber crime" cases, important evidence is found in computers/cell phones, for example. In cases of divorce, murder, kidnapping, organized crime, terrorist operations, counterfeit currency etc.

Cyber law is of utmost importance as it touches all aspects of transactions and activities related to the Internet, the World Wide Web and cyberspace.

WORLD AND CYBER LAW- The Great Firewall of CHINA monitors every moment in cyberspace and prevents any objectionable material from being published. China has a hold on every material that is dangerous or harmful to the Chinese government.

BRAZIL is considered the world's largest airport for hackers. IRAN is also a dangerous country for netizens. They also have a crime police unit for crime in cyberspace.

INDIAN CYBER LAWS - India's first cyber crime happened in 1992 when the first polymorphic virus was released. The *Yahoo vs Akash Arora (1999)* case was one of the earliest instances of cybercrime in India. Yahoo INC v. Akash Arora' is a landmark Indian case on 'cybersquatting'. This case marks the first time the Delhi High Court declared that a domain name has the same level of protection as a trademark. This is important because it depicts a central issue of IP law concerning passing-off under Indian trademark law.[10]

Telangana is the top region in the number of cyber crimes in India and top 5 regions others are Uttar Pradesh, Karnataka, Maharashtra and Assam. In India, cyber laws are contained in the Information Technology Act, 2000 ("IT Act"), which came into force on October 17, 2000. The main objective of the Act is to provide legal recognition to electronic commerce and facilitate electronic filing. Records with the government.

No existing law has given any legal validity or sanction to the activities in cyberspace. For example, most users use the net for email. Yet till date, email ID is not "legal" in our country. There is no such law in the country, which gives legal validity and approval to email. Courts and Judiciary in our country have been reluctant to give judicial recognition to the validity of email in the absence of any specific law enacted by the Parliament. In such a situation, the need for cyber law has arisen.

But still the IT Act specifies the acts which have been made punishable. The Indian Penal Code, 1860 has also been amended to cover cyber crimes. Various offenses related to internet which have been made punishable under Information Technology Act 2000 and Indian Penal Code 1860 are as follows -

Cyber Crime Under Information Technology Act 2000 -

Tampering with computer source documents - Section 65

Hacking with computer system, altering data - Section 66

Publishing obscene information - Section 67

Unauthorized access to protected system section 70

Violation of secrecy and privacy - Section 72

Publishing false Digital Signature Certificate - Section 73

Cyber Crime Under Indian Penal Code 1860 -

Sending threatening messages by email - IPC Section 503

Sending abusive message by email - IPC section 499

Forgery of electronic record - Section 463 IPC

Fake websites, cyber fraud - IPC section 420

Email Spoofing - Section 463 IPC

Web-jacking - Sec. 383 IPC

Misuse of E-mail - IPC Section 500

Cyber Crimes Under Special Acts - Online sale of drugs under the Narcotic Drugs and Psychotropic Substances Act

Online sale of arms Arms Act

INDIAN CYBER CRIME COORDINATION CENTER- In January 2020, the Indian Cyber Crime Coordination Center (I4C) has been inaugurated by the Ministry of Home Affairs to deal with cybercrime.

[10] https://www.theipmatters.com/post/yahoo-inc-v-akash arora#:~:text='Yahoo%20INC%20v.,off%20under%20Indian%20trademark%20law.

Purpose of coordination centre as follows - To act as a nodal point in the fight against cybercrime. To identify research problems/needs of LEA and to undertake R&D activities in development of new technologies and forensic tools in collaboration with academia/research institutions in India and abroad. Preventing misuse of cyberspace to further the cause of extremist and terrorist groups. Suggest amendments, if necessary, in cyber laws to keep pace with rapidly changing technologies and international cooperation. Coordinating all activities relating to implementation of Mutual Legal Assistance Treaties (MLAT) with other countries relating to cybercrime in consultation with the concerned nodal authority in the Ministry of Home Affairs. This scheme has been implemented all over India. In order to better deal with cybercrime and to implement I4C in a coordinated and effective manner, 14C aims to strengthen the capability of Law Enforcement Agencies (LEAs) and improve coordination between various agencies and LEAs, and that the vision of the scheme is to create an effective framework and ecosystem for prevention, detection, investigation and prosecution of cyber crimes.[11] the plan has the following seven major components-

1. National Cybercrime Threat Analytics Unit
2. National Cyber Crime Reporting Portal
3. Platform for Joint Cyber Crime Investigation Team
4. National Cyber Crime Forensic Laboratory Ecosystem
5. National Cyber Crime Training Center
6. Cyber Crime Ecosystem Management Unit
7. National Cyber Research and Innovation Center.

GOVERNMENT'S EFFORTS TOWARDS DEALING WITH CYBERCRIME- The 'Information Technology Act, 2000' was passed in India whose provisions and the provisions of the Indian Penal Code collectively are sufficient to deal with cyber crimes. Sections 43, 43A, 66, 66B, 66C, 66D, 66E, 66F, 67, 67A, 67B, 70, 72, 72A and 74 of the Information Technology Act 2000 deal with hacking and cyber crimes.

The 'National Cyber Security Policy, 2013' was released by the government, under which the government constituted the 'National Critical Information Infrastructure Protection Center (NCIIPC)' to protect highly sensitive information. Under this, there is also a provision for punishment ranging from 2 years to life imprisonment and punishment or fine.

With a view to develop human resources in the field of information security at various levels, the Government has launched the Information Security Education and Awareness (ISEA) project.

The 'Computer Emergency Response Team (CERT-In)' was set up by the government which is the national level model agency for computer security.

A 'Cyber Swachhta Kendra' has also been set up in the country to deal with cyber crimes in a coordinated and effective manner. It is a part of the Digital India campaign of the Government of India under the Ministry of Electronics and Information Technology (MEIT).

India is coordinating with countries like the US, UK and other contreis to share information and adopt best practices in terms of cyber security.

For inter-agency coordination, the 'Indian Cyber Crime Coordination Centre-I4C' has been set up.

[11] https://theprint.in/india/centre-sent-over-100-crore-phone-messages-to-raise-awareness-on-cyber-crimes/935771/

According to the Seventh Schedule of the Indian Constitution, "Police" and "Public Order" are State subjects. Through their Law Enforcement Agencies (LEAs), States and Union Territories are largely in charge of prevention, detection, investigation and prosecution of crimes including cybercrime. Law Enforcement Agencies (LEAs) prosecute criminals as per the provisions of law.

Whereas, the Central Government supports the efforts of the State Governments by providing guidance and financial assistance through various programs for capacity building. The central government has taken action to increase public awareness of cybercrimes, including issuing alerts and advisories, capacity building and training for law enforcement, prosecutors and judicial officials, as well as the development of cyber forensic techniques.

Programs are run by the Ministry of Electronics and Information Technology (MeitY) to enhance people's understanding about information security. Information security-specific books, movies, and online resources designed for children, parents, and general users.

Major Cases of Cyber Crime in India[12]

- Kotak Mahindra Bank **vs** K. Seetharam Bhatt 14 jan. 2022
- Mahesh Kumar Poddar vs The State Of Jharkhand on 13 May, 2022
- Bablu Kumar Mandal vs The State Of Jharkhand on 15 September, 2022
- Tirth Nath Akash vs State Of Jharkhand on 14 May, 2018
- **SMC Pneumatics (India) Pvt. Ltd. vs. Jogesh Kwatra** CM APPL. No. 33474 of 2016
- **Shamsher Singh Verma v. State of Haryana** 2015 SCC OnLine SC 1242
- **Shreya Singhal v. UOI** (2013) 12 SCC 73

SUGGESSIONS TO THE CYBER CRIME PREVENTION

- Backup all data, systems and ideas - This enables previously stored data to help businesses recover from an unplanned event.
- Implement solid security and keep it up to date - Choose a firewall with features that protect against malicious hackers, malware, and viruses. This enables businesses to identify and respond to threats more quickly.
- Never give personal information to strangers - they can use this information to commit fraud.
- Check Security Settings to Prevent Cyber Crime - A cyber firewall checks your network settings to see if anyone has logged into your computer.
- Using Antivirus Software - Using Antivirus software helps in identifying any threats or malware before they can infect the computer system. Never use hacked software as it can put you at serious risk of data loss or malware attack.
- Protect your information when visiting unauthorized websites - Informers can easily bypass data using phishing websites.
- Use a Virtual Private Network (VPN) - VPN enables us to hide our IP addresses.
- Restrict access to your most valuable data: Create a folder, if possible, so that no one can see confidential documents.

[12] https://indiankanoon.org/search/?formInput=cyber%20crime%20cases

- Keep an eye out for irrelevant or fraudulent messages or emails.
- Make note of the email address and password.
- Do not click on unfamiliar URLs or download unknown apps.
- Stay updated about cyber laws and policies.

The most important part is to have thorough knowledge and awareness about privacy and cyber crimes so that people can be saved from such threats. There should be more education on cyber crimes and online frauds and how to get rid of or deal with them. Cyber literacy should start from the basic level with adequate knowledge about good operational practices. There is a need to be extra vigilant about cyber privacy and security. Proper awareness and education can help in developing good habits and practices while working online with digital tools. There is also a need for strict law enforcement and punishment for criminals. Media intervention for creating public awareness can contribute effectively in bringing about a change in the attitude of people towards gender norms.

CONCLUSION- We are living in a digital age and cyberspace is not limited to anyone's borders rather it covers the whole world. As a result, cybercrime is increasing day by day in all countries including India. The biggest challenge is related to the dynamic nature of cybercrime due to the ongoing development of digital technology. As a result, new methods and techniques of cybercrime have come into vogue.

That's why cyber crime should be given equal importance as other crimes happening in our society whether it is theft, rape, murder etc. Technology solutions have opened up a new world of corporate networking, e-banking and the Internet, which can cut costs and transform complex economic matters into simpler, faster, more efficient and time-saving methods. appeared as a solution. Many criminals, including hackers and crackers, have found ways to tamper with online accounts and have been effective in gaining illegal access to users' computers and stealing important data.

Lastly, though a crime free society may be a dream, efforts should be made to make laws that keep crime to a minimum. Legislators must take extraordinary measures to deter copycats as criminality related to breaking electronic laws will inevitably increase, especially in a society where technology is used more and more. Technology often has two sides and can be used for both good and bad purposes.

Rulers and law makers should make continuous efforts to ensure that technology progresses in a healthy manner and is used for legal and ethical economic growth rather than criminal activities.

In an increasingly technology-dependent world, criminal activities related to electronic and internet platforms are on the rise, targeting women as well. There should be specific provisions in the laws to punish such criminals with strict action. Tackling cyber crime against women requires greater awareness and knowledge about cyber practices, privacy protection and legal support.

REFERENCES :

1. Prof. R.K.Chaubey, “An Introduction to Cyber Crime and Cyber law”, Kamal Law House, 2012
2. Cyber Ctimes and Laws, Dr. US Pandey, Dr. V.Kumar, Dr. HP, Himalya Publshing House- 2017 p-15
3. K. Chethan, “One cybercrime in India every 10 minutes - Times of India,” The Times of India, 22- Jul-2017.

4. Rahman, Rizal. (2012). Legal jurisdiction over malware-related crimes: From theories of jurisdiction to solid practical application. Computer Law & Security Review 28 (2012) 403-415.
5. United Nations International Residual Mechanism for Criminal Tribunals. (2003). Three Media Leaders convicted for Genocide .
6. S. J. Juneidi, "Council of Europe Convention on Cyber Crime"
7. "Convention on Cybercrime European Treaty Series - No. 185." Council of Europe XI-2001.
8. Cyber Crime in India: A Comparative Study M. Dasgupta, 2009

INTERNET RESOURCES

1. http://en.wikipedia.org/ wiki/Security
2. https://goosevpn.com/blog/origin-cybercrime
3. https://www.swierlaw.com/faqs/what-are-the-three-types-of-cyber-crimes-.cfm
4. https://intellipaat.com/blog/what-is-cybercrime/
5. http://ijiet.com/wp-content/uploads/2013/07/32.
6. https://theprint.in/india/centre-sent-over-100-crore-phone-messages-to-raise-awareness-on-cyber-crimes/935771/
7. https://clearinsurance.com.au/10-biggest-cyber-attacks-in-history
8. https://www.coe.int/en/web/cybercrime/the-budapest-convention
9. https://www.theipmatters.com/post/yahoo-inc-v-akash arora#:~:text='Yahoo%20INC%20v.,off%20under%20Indian%20trademark%20law.
10. http://en.wikipedia.org/wiki/Data-security
11. http://www.cyberlawsindia.net/
12. http://www.hindustantimes.com/