Volume 10, May 2020 ISSN 2581-5504

"Cyber Crime"

Kashika Mahajan
Bharati Vidyapeeth New Law College,
Pune

INTRODUCTION

The term crime is not new to the world. It is as old as human society but the term cybercrime is a new form of crime that has taken place and is playing a devastating role in Modern India. It is growing at an alarming rate. One can define cybercrime as unlawful or a criminal activity that takes place over computer, internet and other technologies that are related to information technology. The activities like attacking on Information center Data System, theft, child pornography built images, online transaction fraud, internet sale fraud and also deployment in internet malicious activities such as virus, worm and third party abuse like phishing, email scams etc. Crime is both social and economic phenomenon. Many pre- historic books and methodologies talk about this. Since the time immemorial theft, harassment, rape and spying etc. were committed by an individual. Taking the example from Mahabharata – how Draupadi was harassed by Dushasana. That was a crime. Kautilya's Arthashastra composed around 350 BC, viewed as a bona fide authoritative treatise in India, talks about the fluctuated violations, security activities to be taken by the rulers, potential wrongdoings during a state and so on and furthermore advocates discipline for the rundown of some specified offences. Different kinds of punishments are prescribed for listed offences and therefore the concept of restoration of loss to the victims. The usage of computer, computer technologies and network is growing day by day. Human has got completely dependent on computers. As we know that the nature of internet is anonymous; one can easily conceal its identity and can commit cybercrime. Computer these days have become an evil base for committing a cybercrime. It is darkest side of internet. One needs to be very cautious while using computer and technologies involving information technology. The moment one takes his eyes away from internet, his computer will be hacked or some kind of virus will attack the software. Every day when we read a newspaper in the morning with a cup of tea or open any social media site we come across the news of cybercrime. Cybercrime is the biggest threat and disadvantage of cyber space.

DEFINITION

The world cyber-crime has not been defined anywhere neither in IT ACT, 2000 nor in amendment of IT ACT, 2008 and also not no legislation of India talks about it. It's Indian Penal Code 1860 that deals with crimes and different types of punishment. The IT Act talks about computer, computer network, data, information etc. basically all the ingredients that form the part of cyber-crime.

- **Dr. Debarati Halder and Dr. K. Jaishankar** define cybercrimes as: "Offences that are committed against individuals or groups of individuals with a criminal motive to

Volume 10, May 2020 ISSN 2581-5504

intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)"[1]

- The **oxford Dictionary** defined the term cybercrime as "Criminal activities carried out by means of computers or the Internet."[2]
- According to **Manish Lunker**, - "Computer or Cyber armies are considered as illegal, unethical, or unauthorized behavior of people relating to the automatic processing and transmission of data, use of Computer systems and Networks"[3]
- According to the **website of Crime Investigation Department, Andhra Pradesh State Police**, "Cybercrime means Unlawful acts wherein the computer is either a tool or a target or both."[4]
- **Professor S.T. Viswanathan** has given three definitions in his book The Indian Cyber Laws with Cyber Glossary is as follows –

1 Any illegal action in which computers are the tool or object of the crime i.e. any crime, the means or purpose of which is to influence the function of a computer,

2 Any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator, by intention, made or could have made a gain,

3 Computer abuse is considered as any illegal, unethical or unauthorized behavior relating to the automatic processing and transmission of data.[5]

EVOLUTION AND HISTORY

Where Does Cyber Crime Came From: This question might have clicked in our mind number of times. Today we'll be getting the answer of this. Surprising it came into existence before internet came into being. Cybercrime was related to data theft. Aren't to you surprised.

HISTORY

The computer was not invented for any entertainment purpose but to solve our problems related to calculations as it was very difficult for a man to do such huge calculations. But today it is used for several purposes. It will be right to say that 21st century is the era of digitization; internet also

[1] http://www.ripublication.com/irph/ijict_spl/ijictv4n3spl_06.pdf (Accessed on 4th January, 2016)
[2] http://www.oxforddictionaries.com/definition/english/cybercrime (Accessed on 4th January, 2016)
[3] Lunker Manish : Cyber Laws: A Global Perspective pg. 2(An article from Internet) See http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN005846.pdf.
[4] 9 http://www.cidap.gov.in/mainwccrime.aspx See also, same definition appeared on the web site of Cyber Crime Police Station, Banglore, Karnataka, http://www.Cyberpolicebangalore.nic.in/Cybercrimes.htm
[5] S.T. Viswanathan, The Indian Cyber Laws with Cyber Glossary, 2001, p. 81

Volume 10, May 2020 ISSN 2581-5504

came into being in 21st century only. The first computer resembling today's modern machines was designed from 1833-1871 by Charles Babbage who is also known as the father of computers. For the very first time when computer was invented it was too big that it requires a space equivalent to a room. It was very expensive and everyone couldn't afford it. It was very difficult for the one to use computer until IBM came into existence wherein it introduced its stand-alone "personal computer" in 1981. By that time few got the knowledge of how to use it. The Personal computers became less expensive and grow to be household object at the beginning of 21st century in India. The Internet changed into first began via the US department of defence, after World War II with the concept to have a network that could paintings in the occasion of catastrophe or conflict and securely transmit records. The First Network becomes called ARPANET, with the development of Transmission Control Protocol/Internet Protocol, World Wide Web and Hypertext the net grow to be rage everywhere in the world.

With the boom of Internet the pleasant and range of information grew. However at that factor nobody expected the opportunities' the net goes to provide the technology savvy criminals. Undoubtly it has improved our lives and has made everything easier. Man has been completely dependent on technologies and can't think their life beyond it. While computer technology has opened doors to enhanced conveniences for many, this same technology has also opened new doors for criminals.

In India the internet services started by the state-owned Videsh Sanchar Nigam Limited in year 1995 and in 1998 the government has ended the monopoly of VSNL and market is opened to private operators too. Now India is the 2nd largest country in the world to provide the services of internet after China.

EVOLUTION OF CYBER CRIME

- While cybercrime existed before this, the first main wave of cyber-crime got here with the proliferation of email at some point of the late 80's. It allowed for a number of scams and/or malware to be added for your inbox.
- The next cybercrime that came was in the of 90's .At the time there had been a mess to choose from, many greater than today, and most had been vulnerable to viruses. Viruses had been delivered through Internet connections each time questionable web sites had been visited. Some precipitated your laptop to run slow, others may have prompted annoying pop-up advertising to crowd your display or redirect you to the nastiest porn sites.
- Cybercrime really began to take off in the early 2,000's whilst social media got here to life. The surge of people putting all the records they may into a profile database created a flood of personal records and the upward thrust of ID theft. Thieves used the statistics in some of

Volume 10, May 2020 ISSN 2581-5504

approaches including getting access to bank accounts, setting up credit score playing cards or other economic fraud.

- The latest wave is the status quo of an international criminal enterprise totaling nearly half-trillion bucks annually. These criminals operate in gangs, use well-established strategies and target something and everybody with a presence at the web.

First Cyber Crime

The principal recorded cybercrime occurred in the year 1820. That isn't astonishing considering the way that the math device, which is believed to be the most punctual type of a PC, has been around since 3500 B.C., in India, Japan and China. The time of present day PCs, be that as it may, started with the expository motor of Charles Babbage. In 1820, Joseph-Marie Jacquard, a material maker in France, created the loom. This gadget permitted the redundancy of a progression of steps in the weaving of unique textures. This brought about a dread among Jacquard's workers that their customary business and vocation we're being undermined. They submitted demonstrations of treachery to discourage73 Jacquard from further utilization of the new innovation. This is the main recorded cybercrime.

CHARACTERISTICS OF CYBER CRIME

1. **PEOPLE WITH SPECIALIZED KNOWLWDGE**: Cyber-crime can only be committed by a person who has specified knowledge about cyber space. One should have deep knowledge about internet, computer and computer network. It's very difficult for the police to find a hacker, once the crime is committed.
2. **GEOGRAPHICAL CHALLENGE**: There is no barrier in cyber space. One can easily express their thoughts and views over internet. Social media is becoming a platform where maximum cyber-crimes are committed. A person can commit cyber by sitting anywhere in the world. For example a hacker sitting in India hack in the system placed in United States.
3. **LACK OF AWARENESS AMONG PEOPLE**: Many a times, the victim affected by cybercrime is unaware of its occurrence because of lack of adequate skill and know-how in handling the computer system.
4. **VIRTUAL WORLD**: The act of cybercrime is committed over cyber space. Each and every activity as well as criminal activities are happening over the virtual world. Crime over the computer, computer network and internet is very popular nowadays.
5. **COLLECTION OF EVIDENCE**: It's very difficult to collect evidence of the crime committed over the virtual world. As hacker can easily hide his real identity. The detection of cybercrimes requires hi-tech skill which the investigators generally lack.

Volume 10, May 2020 ISSN 2581-5504

6. **MAGNITUDE OF CRIME UNIMAGINABLE**: One never thought that crime will ever take the shape like this. All thanks to cyber space that in every field is possible. These crimes can cause permanent injury and damage to an individual or society at large.
7. **NO VIOLENCE IS INVOLVED**: The cybercrime does not involve any violence, but is rather an outcome of greed, mischief and exploiting the weakness of the victim.

FEATURES OF CYBER CRIME

1. It is an unlawful act.
2. It has no boundaries.
3. Computer plays an important role in cybercrime. It is a tool to commit target.
4. It can cause permanent damage or injury to an individual or society at large.
5. It is a criminal activity.
6. It is an illegal activity done with a malicious purpose.
7. It's very difficult to collect evidences once the crime is committed.
8. It's not always necessary that loss will be in terms of money only.

NATURE AND SCOPE OF CYBER CRIME

The nature of crime depends upon the nature of society. So scope, definition and nature of crime changes from time to time. Crimeless society is a myth and crime cannot be segregated from a society. It has become a global phenomenon. Cybercrime is a crime on the Internet which includes hacking, terrorism, fraud, gambling, cyber stalking, cyber theft, cyber pornography, flowing of viruses etc.

The report of the United Nations[6] stated that more than 50 % of the websites in the US, Canada and European countries have experienced breach of security and threats of cyber terrorism which threw a serious challenge before the law enforcement agencies. A new trend that has developed in recent years is that the militants are going for terror training. The Internet has become a key teaching tool for militants who are using it to educate recruits in cyber terrorist's training camps.

Gabriel Weimann, an Internet and security expert who teaches in the University of Mainz in Germany and has studied militant's use of website for nearly a decade, while addressing the Internet security personnel said that, "website and chat room used by militant Islamic Groups like Al-Qaida are not only used for dissemination of propaganda but also for terrorist education.

[6] U.N. Report on International Review of Criminal Policy and Prevention & Control of Computer Crime (October, 2005.)

Volume 10, May 2020 ISSN 2581-5504

Al-Qaida has launched a practical website that shows how to use weapons, how to carry out kidnapping and how to use fertilizers to make a bomb."[7]

The computer related crime has already become an area of serious concern for most of the countries of the world, and India is no exception to it. The prime factor that has to be taken into consideration while deciding whether a particular computer related activity be reckoned as cybercrime is that a distinction must be drawn between what is unethical and what is illegal. It is only when an activity is truly illegal; it should be treated as crime and the prosecution of the offender must be sought. Therefore, criminal law should be implemented with restraint in determination of cases which relate to cyber law.[8]

Meaning of Mens Rea –

- 'Mens rea' refers to the 'mental element of an offence' and is an essential element of a crime.
- Cyber-crimes being different from the conventional crimes as they are committed in the electronic medium;
- Mens rea is not a requirement but is rather a general rule under the penal provisions of the IT Act.
- The element of mens rea in Cyber-crimes is that the offender must have been aware at the time of causing the computer to perform the function that the access thus intended to be secured was unauthorized.

Meaning of Actus reus-

It is a criminal act that was the result of voluntary bodily movement. This describes a physical activity that harms another person or damages property.

Actus reus unaccompanied with mens rea is not a crime.

- Actus reus + Mens rea = Crime
- Actus reus + No Mens rea = No Crime
- No Actus reus + Mens rea = No Crime[9]

Actus res and Mens rea are two important ingredients in law. Whenever the crime is committed these two are taken into consideration.

The essence of criminal law has been said to lie in the maxim- "actus non facit reum nisi mens sit rea." Bishop writes: ' "There can be no crime large or small, without an evil mind.[10]

[7] Gabriel Weimann was addressing a Conference on Internet Security at the headquarters of Germany's Federal Police Office, as reported in the Times of India, Delhi edition, dated November 23, 2007.
[8] Dr. R.K. Raghvan, "Salutations", CBI Bulletin, Vol. VIII No. 2, February, 1999, p. 4.
[9] https://shodhganga.inflibnet.ac.in/bitstream/10603/7829/12/12_chapter%203.pdf

Volume 10, May 2020 ISSN 2581-5504

THREAT MEDIUM / ATTACK VECTORS

1. **VIRUS:** Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They ordinarily influence the information on a PC, either by changing or erasing it.
2. **WORMS:** Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory.
3. **BOTNETS:** The word 'botnet' is a combination of two words, 'robot' and 'network.' Here, a cybercriminal who performs the role of a botmaster uses Trojan viruses to breach the security of several computers and connect them into a network for malicious purposes. Each computer on the network acts as a 'bot' and is controlled by a scammer to transmit malware or spam or malicious content in order to launch the attack. A botnet is also known as a Zombie Army as the computers involved are being controlled by someone other than their owner.
4. **ROOTKITS:** A rootkit is malicious software that allows an unauthorized user to have privileged access to a computer and to restricted areas of its software. A rootkit may contain various malevolent devices, for example, keyloggers, banking accreditation stealers, secret key stealers, antivirus disablers, and bots for DDoS assaults.
5. **Data diddling:** This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed. Electricity Boards in India have been victims to data diddling programs inserted when private parties were computerizing their systems. The NDMC Electricity Billing Fraud Case that took place in1996 is an example this.

6. **Phishing Scams**: It is a fraudulent attempt to obtain sensitive information like password, username, bank account numbers, and credit and debit card numbers. Scammers disguise people very people either by saying they want to update the account of the holder or they are facing some technical problem for which they need their personal information. It can be done through phone numbers, text message, emails and via social media websites like whatsapp, instagram, facebook etc.

7. **Malware**: It is software that is specially made to disrupt, damage and to gain unauthorized access to computer software. The common types of malware include spyware, Trojan computer viruses etc. They will net get into the computer and create chaos into the system and steal all the necessary information.
8. **Ransomware**: A type of malicious software designed to block access to a computer system until a sum of money is paid.

[10] Criminal Law, 9th Edition (1930) 287.

Volume 10, May 2020 ISSN 2581-5504

9. **Hacking of Social Media & Spamming**: social media hacking means when the hacker hack the username and password and use that in a wrong way.

Spamming means sending unwanted or irrelevant messages over the internet. These are sent to many people at a same time. It can be sent for advertisement purpose, phising, spreading malware etc.

KINDS OF CYBER CRIME

1. **Computers as a Tool of Cybercrimes:** In this category of cybercrime, computer is used as the means of committing cybercrimes. Where individual is the main target of Cybercrime, the computer can be considered as the tool rather than the target. For committing this type of cybercrimes, the role of computer is same as played by the telephone in telephone fraud.
   Let's see what heads come under this:
   - Credit Cards Fraud
   - Electronic funds transfer fraud
   - Fraudulent use of ATM cards and accounts
   - E-Commerce fraud
   - Telecommunications fraud
   - Stock transfers fraud etc.

2. **Computers as a target for committing Cybercrimes:** Earlier we discussed how computer is used as tool now we see how it acts as a target. In this the trespasser attacks the computer by breaking into it or attacking it from outside These types of crimes are committed by specific group of people as it requires technical knowledge. The main purpose of committing these cybercrimes is to directly cause damage to a computer system or to access the important data stored in a computer.
   It includes following types of cybercrimes:
   - Intellectual Property Theft
   - Marketable information theft
   - Theft of data/information
   - Destroy of computer, computer system or computer networks
   - Unlawful access to government records and criminal justice etc.

TYPES OF CYBER CRIME

The list of cybercrime is inexhaustible. So here we will discuss few of them:

Volume 10, May 2020 ISSN 2581-5504

1. **Phishing Scams**: It is a fraudulent attempt to obtain sensitive information like password, username, bank account numbers, and credit and debit card numbers. Scammers disguise people very people either by saying they want to update the account of the holder or they are facing some technical problem for which they need their personal information. It can be done through phone numbers, text message, emails and via social media websites like whatsapp, instagram, facebook etc.

There were phishing attempts over ICICI Bank, UTI Bank, HDFC Bank, SBI etc. in which the Modus operandi was similar. It was reported that a large number of customers of these banks had received emails, which have falsely been misrepresented to have been originated from their bank.[11]

ILLUSTRATION: A got email from B, stating that A has won a lottery of RS.10, 000. To get the money transferred into his account he need to his account details.

- SECTION: 420 &463 IPC, 43 of IT ACT 2000
- OFFENCE: Bogus websites, cyber frauds & E -mail spoofing, Damage to computer, computer system, etc.
- PENALITY: Shall be punished with an imprisonment of either description for a term which may extend to seven years and shall also be liable for a fine & compensation not exceeding one crore rupees to the person so affected.

2. Malware: It is software that is specially made to disrupt, damage and to gain unauthorized access to computer software. The common types of malware include spyware, Trojan computer viruses etc. They will net get into the computer and create chaos into the system and steal all the necessary information.

CASE LAW**:** Syed Asifuddin and Ors. V. The State of AP. & Anr.2005CriLJ4314

The court held that such manipulation amounted to tampering with computer source code as envisaged by section 65 of the Information Technology Act, 2000.

ILLUSTRATION: Sometimes we open our computer or tablet virus sign appears and immediately our computer hangs or we open any website the same thing we witness. This is the example of malware.

- SECTION: 43 & 65 of IT ACT 2000
- OFFENCE: Damage to computer, computer system, etc. & Tampering to computer source documents.

[11] http://www.crimes-of-persuasion.com/Crimes/Business/nigerian.htm

Volume 10, May 2020 ISSN 2581-5504

- PENALITY: Compensation not exceeding one crore rupees to the person so affected & Imprisonment up to three years, or with fine which may extend to upto two lakh rupees, or both.

3. **E-MAIL Bombing**: E-mail bomb is form of internet abuse. Abuse here doesn't mean sending obscene images but sending large number of emails in an attempt to overflow the mail box. This can be done by ways: a) mass mailing b) list linking c) zip bomb.

EXAMPLE: Spam e-mails,

- SECTION: 43 of IT ACT 2000
- OFFENCE: Damage to computer, computer system, etc.
- PENALITY: Compensation not exceeding one crore rupees to the person so affected.

4. Hacking of Social Media & Spamming: social media hacking means when the hacker hack the username and password and use that in a wrong way.

Spamming means sending unwanted or irrelevant messages over the internet. These messages are sent to many people at a same time. It can be sent for advertisement purpose, phising, spreading malware etc.

ILLUSTATION: Many times one has noted friends putting their story on instagram or facebook that their id got hacked, report this account. Which means someone else has made an account putting the same usename as theirs?

- SECTION: 43 & 66 IT ACT 2000, 378, 425 IPC 1860.
- OFFENCE: Damage to computer, computer system, etc. & Hacking with computer systems, data alternatives etc. & Data theft
- PENALITY: Compensation not exceeding one crore rupees to the person so affected. & Imprisonment for a term which may extend to three years or with a fine which may extend to five lakh rupees or with both. &

The maximum punishment for theft is imprisonment of up to 3 years or a fine or both. & the maximum punishment for mischief as per section 426 of the IPC is imprisonment of up to 3 months or a fine or both.

5. Cyber defamation: It refers to injury caused to a person by harming his\her reputation infront of a third person through digitization; it can be in a form of material published online or uploading a video on YouTube etc. . It is not a criminal act but a tort.

Volume 10, May 2020 ISSN 2581-5504

CASE LAW: Google India Private Ltd vs M/S. Visakha Industries on 10 December, 2019[12]

ILLUSTRATION: If A put a post on a social media stating that B has committed adultery and also B hits his wife daily. A did also this because he has some personal differences with B. This is a case of cyber defamation.

- SECTION: 499 IPC
- OFFENCE: Sending defamatory messages by e-mail.
- PENALITY: Punishable under sec 500 of IPC with a simple imprisonment upto 2 years or fine or both.

6. Child pornography: It is also known as child abuse over web. It refers to uploading of obscene images of minor over internet. It is a form child sexual exploitation. It is illegal and if someone find child abuse images should immediately report to the police.

The POCSO Act through inclusive of demise penalty for irritated sexual attack on youngsters, besides imparting stringent punishments for other crimes in opposition to minors. (Amendment 2019)

CASE LAW: Avnish Bajaj vs State on 29 May, 2008**[13]**

Maqbool Fida Husain vs Raj Kumar Pandey (Along With Crl. ... on 8 May, 2008)**[14]**

ILLUSTRATION: ABC is porn site on internet that uploads pictures of minor sexual abuse.

- SECTION: 67B of IT Act 2000 & 292 and 294 of the IPC 1860
- OFFENCE: Abusing children online. &

Any person who, inter alia, sells, distributes, publicly exhibits or in any manner puts into circulation or has in his possession any obscene book, pamphlet, paper, drawing, painting, representation or figure or any other obscene object.

- PENALITY: Imprisonment for a term which may extend five years and with a fine which may extend to ten lakh rupees and in the event of a second or subsequent convictions with imprisonment of either description for a term which may extend to seven years and also with a fine which may extend to ten lakh rupees & Shall be punishable on a first conviction with imprisonment of either description for a term which may extend to 2 years, and with fine which may extend to Rs. 2,000 and, in the event of a second or

[12] https://indiankanoon.org/doc/97017195/
[13] https://indiankanoon.org/doc/309722/
[14] https://indiankanoon.org/doc/1191397/

Volume 10, May 2020 ISSN 2581-5504

subsequent conviction, with imprisonment of either description for a term which may extend to 5 years, to be accompanied by a fine which may extend to Rs. 5,000.

7. Online harassment: It means bulling done over virtual world. In this basically stalker targets, threatens, insults, abuse a particular person. Cyber stalking, online impersonation, catfishing, doxxing, swatting, trolling and revenge porn, etc. are types of online harassment.

ILLUSTRATION: If X uploads MMS of Z to take revenge from Z.

- SECTION: 66A of IT Act 2000 &503 IPC
- OFFENCE: Sending offensive messages through communication services etc. & Sending threating messages by e-mail.
- PENALITY: Imprisonment for a term which may extend to three lakh rupees and with fine. & Shall be punished by simple imprisonment for a term which may extend to one year, or with a fine, or both.

8. Electronic Money Laundering: Money generated in large volumes illegally must be laundered before it can be spent or invested. There are several common types of money laundering, including casino schemes, cash business schemes, smurfing schemes, and foreign investment/round-tripping schemes.

9. Software Piracy: Nowadays, thanks to the internet, you can find almost any movie, song or software for free online. Software piracy is the unauthorized use and distribution of computer software. Even though using pirated material may seem good because it's free, it comes with a range of risks. These risks include: Trojans, viruses, worms and other forms of malware.

ILLUSTRATION: -If A purchases from B Microsoft office and he sells him pirated version with the passage of time it will start corrupting the computer system.

- Two friends Malav and Tushar had a heated argument over one girl, Kiara whom they both liked. When the girl, asked to choose, she chose Malav over Tushar, Tushar decided to get even. On 3rd September, he sent Malav a spoofed e-card, which appeared to have come from Kiara's mail account. The e-card actually contained a Trojan. As soon as Malav opened the card, the Trojan was installed on his computer. Tushar now had complete control over Malav's computer and proceeded to harass him thoroughly.

- SECTION: 66 of IT Act 2000
- OFFENCE: Hacking with computer systems, data alternatives etc.
- PENALITY: Imprisonment for a term which may extend to three years or with a fine which may extend to five lakh rupees or with both.

Volume 10, May 2020 ISSN 2581-5504

10. Identity Theft: Identity theft is one of the most common types of cybercrime. The main reason identity theft occurs is with the view of creating fraud for financial gains. Criminals usually steal identity information of others such as credit card information, addresses, email addresses and more. With this information they can pretend to be someone else and create new bank accounts.

ILLUSTRATION: If A pretends to be B's son(X) and takes all information of his bank accounts.

- SECTION: 66D of IT Act 2000, & 419 IPC, 1860
- OFFENCE: Cheats by personating by using computer resource. & Cheating by personation
- PENALITY: Imprisonment for a term which may extend to three years and shall be liable to a fine which may extend to rupees one lakh. &

11. Cyber terrorism: It's a new form of terrorism that has surpassed traditional terrorist attacks. It refers to use of internet to conduct violent acts which will result into bodily harm, loss of life in order to achieve political and ideological gains. This word has a very broad meaning.

- SECTION: 66F of IT Act 2000
- OFFENCE: Cyber terrorism
- PENALITY: Imprisonment for a term which may extend to imprisonment for life.

12. **Cyber Pornography**: Pornography means showing sexual acts in order to cause sexual excitement. The definition of pornography also includes pornographic websites, pornographic magazines produced using computer and the internet pornography delivered over mobile phones. Case law: DPS MMS scandal 2004.

ILLUSTRATION: If A launches a website in XYZ country where pornography is banned and still is using that website to upload explicit content. It means he has omitted a cybercrime.

- SECTION: 66E, 67, 67A of IT Act 2000 & 292 and 294 of the IPC 1860
- OFFENCE: Publishing obscene images; publishes or transmits unwanted images.; publishes or transmits sexually explicit material. & any person who, inter alia, sells, distributes, publicly exhibits or in any manner puts into circulation or has in his possession any obscene book, pamphlet, paper, drawing, painting, representation or figure or any other obscene object.
- PENALITY: Imprisonment for a term which may extend to three years or with a fine not exceeding two lakh rupees or with both & imprisonment for a term which may extend three years and with a fine which may extend to five lakh rupees and in the event of a second or subsequent convictions with imprisonment of either description for a term which may extend to five years and also with a fine which may extend to five lakh

Volume 10, May 2020 ISSN 2581-5504

rupees; & imprisonment of a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend seven years and also with a fine which may extend to ten year; & shall be punishable on a first conviction with imprisonment of either description for a term which may extend to 2 years, and with fine which may extend to Rs. 2,000 and, in the event of a second or subsequent conviction, with imprisonment of either description for a term which may extend to 5 years, to be accompanied by a fine which may extend to Rs. 5,000.

13. Salami attacks: These attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed.

ILLUSTRATION: A bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say Rs. 5 a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount of money every month.

- SECTION: 66B of IT Act 2000 & 411 of the IPC, 1860
- OFFENCE: Retains any stolen computer resource or communication device. & Dishonestly receiving any stolen property.
- PENALITY: Imprisonment for a term which may extend to three years or with a fine which may extend to one lakh rupees or with both & imprisonment of either description for a term of up to 3 years or with fine or with both.

14. Forgery: Computers, printers and scanners are used to currency notes, postage and revenue stamps, mark sheets etc. These are made using computers, and high quality scanners and printers. It is banned in India.

ILLUSTRATION: If A commits forgery by copying the sign of B who is very rich businessman. A uses the sign for some illegal attack.

- SECTION: 73& 74 of IT Act 2000 & 463, 465 and 468 IPC 1860
- OFFENCE: Publishing false digital signature & Forgery for the purpose of cheating
- PENALITY: Imprisonment for a term which may extend ten years or with a fine which may extend to one lakh rupees or with both. &

IPC prescribes punishment for forgery for the purpose of cheating and provides a punishment of imprisonment of either description for a term which may extend to 7 years and also a fine**.**

15. Intellectual Property crimes: These include software piracy, copyright infringement, trademarks violations, theft of computer source code etc. In other words this is also referred to as cyber squatting.

Volume 10, May 2020 ISSN 2581-5504

CASE LAW: Satyam VS Siffy 2004 [15]is the most broadly known case. Bharti Cell Ltd. documented a case in the Delhi High Court that a few digital vagrants had enlisted area names, for example, barticellular.com also, bhartimobile.com with System arrangements under various imaginary names. The court coordinated System Arrangements not to move the space names being referred to any outsider and the issue is sub-judice.

16. Sale of illegal articles: This would include sale of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by using email communication. E.g. many of the auction sites even in India are believed to be selling cocaine in the name of 'honey'.

ILLUSTRATION:

- SECTION: Narcotic Drugs and Psychotropic Substances (NDPS) Act, 1985
- OFFENCE: Online sale of Drugs

WHO COMMITS CYBER CRIME?

2. **Insiders** – Discontented employees and ex-employees, spouses, lovers.
3. **Hackers** – Enter into networks with malicious intent.
4. **Virus Writers** - Cause serious threats to networks and systems worldwide.
5. **Foreign Intelligence** - Use cyber tools as part of their Services for spying activities and can give rise to the biggest threat to the security of another country.
6. **Terrorists** - Use to formulate plans, to raise funds, propaganda.

SOME RELEVANT IPC SECTIONS THAT LINKED TO CYBER CRIME

- **Sections 292 and 294 of the IPC :**

These provisions could also be relevant for offences of the character defined under sections 67, 67A and 67B of the IT Act. Section 292 of the IPC offers that any person who, inter alia, sells, distributes, publicly exhibits or in any way places into movement or has in his ownership any obscene book, pamphlet, paper, drawing, painting, representation or determine or every other obscene item in anyway will be punishable on a first conviction with imprisonment of both description for a term which may additionally amplify to 2 years, and with excellent which may extend to Rs. 2,000 and, in the event of a 2nd or subsequent conviction, with imprisonment of both description for a term which may additionally enlarge to 5 years, to be followed through a quality which may additionally amplify to Rs. 5,000.

[15] https://indiankanoon.org/doc/1630167/

Volume 10, May 2020 ISSN 2581-5504

Section 294 of the IPC provides that any person who, to the annoyance of others, does any obscene act in any public vicinity, or sings, recites or utters any obscene tune, ballad or phrases, in or near any public place, shall be punished with imprisonment of both description for a time period which may also make bigger to a few months, or with nice, or with each.

- **Section 354A of the IPC:**

Individuals posting lustful remarks via web-based networking media are subject under this law and can be rebuffed with one-year detainment and fine.

Also, posting/informing content identified with sex entertainment against the desire of a Women or mentioning sexual favors are deserving of a fine alongside three years of detainment under a similar arrangement.

- **Section 354C of the IPC:**

This demonstration manages voyeurism which is a criminal offense under both the IPC and the IT Act. It manages situations where a man, without the assent of Women, catches a picture/video of her occupied with a private demonstration. Such a demonstration is deserving of one to three years of detainment alongside a fine. This arrangement can be alluded to particularly in situations when the Women don't &39; hope to be seen by the charged.

- **Section 354D of the IPC:**

This arrangement of the IPC manages what is usually alluded to as " web based following & quot; The arrangement covers the grounds of a situation where an endeavor to contact a Women is made by means of the web, email or some other type of electronic correspondence with the goal of building up close to home association regardless of her obvious lack of engagement. Such a demonstration is culpable with three years of detainment on the principal tally followed by five years of detainment on the second include the two of which are notwithstanding a money related fine.

- **Section 378 of the IPC** :

It is relating to "theft" of movable property will apply to the robbery of any facts, on-line or otherwise, on the grounds that phase 22 of the IPC states that the words "movable belongings" are supposed to encompass corporeal assets of every description, besides land and matters attached to the earth or completely fastened to whatever that is attached to the earth. The most punishment for robbery underneath section 378 of the IPC is imprisonment of up to 3 years or an exceptional or each.

Volume 10, May 2020 ISSN 2581-5504

- **Section 424 of the IPC**:

It states that "whoever dishonestly or fraudulently conceals or removes any property of himself or every other character, or dishonestly or fraudulently assists in the concealment or removal thereof, or dishonestly releases any call for or declare to which he's entitled, shall be punished with imprisonment of both description1 for a term which may additionally extend to 2 years, or with exceptional, or with both." This aforementioned segment may also observe to records theft. The most punishment underneath section 424 is imprisonment of up to two years or a quality or both.

- **Section 425 of the IPC** :

It deals with mischief and states that "whoever with intent to cause, or knowing that he is likely to cause, wrongful loss or damage to the public or to any person, causes the destruction of any property, or any such change in any property or in the situation thereof as destroys or diminishes its value or utility, or affects it injuriously, commits mischief". Needless to say, damaging computer systems and even denying access to a computer system will fall within the aforesaid section 425 of the IPC. The maximum punishment for mischief as per section 426 of the IPC is imprisonment of up to 3 months or a fine or both.

- **Section 411 of the IPC** :

It too prescribes punishment for dishonestly receiving stolen property and is worded in a way that is nearly equal to segment 66B of the IT Act. The punishment beneath phase 411 of the IPC is imprisonment of both descriptions for a time period of up to 3 years, or with best, or with each.

- **Section 419 of the IPC**

It additionally prescribes punishment for 'dishonest via personation' and offers that any man or woman who cheats by personation will be punished with imprisonment of both description for a term which can also increase to three years or with a pleasant or with each. A individual is said to be responsible of 'cheating by personation' if such person cheats via pretending to be a few different individual, or by knowingly substituting one character for every other, or representing that he or every other man or woman is someone aside from he or such other character surely is.

- **Sections 463, 465 and 468 of the IPC** :

These provisions are coping with forgery and "forgery for the cause of dishonest", can also be applicable in a case of identity robbery. Section 468 of the IPC prescribes punishment for forgery for the motive of dishonest and gives a punishment of imprisonment of either description for a time period which can also enlarge to 7 years and additionally an excellent. Forgery has been described in section 463 of the IPC to mean the making of a false document or part thereof with

Volume 10, May 2020 ISSN 2581-5504

the reason to motive harm or damage, to the general public or to any person, or to support any declare or title, or to reason any person to part with property, or to enter into any express or implied contract, or with purpose to dedicate fraud or that fraud may be devoted.

In this context, reference may also be made to phase 420 of the IPC that provides that any individual who cheats and thereby dishonestly induces the character deceived to supply any property to any individual, or to make, regulate or spoil the whole or any a part of a valuable safety, or something that's signed or sealed, and which is able to being transformed into a treasured safety shall be punished with imprisonment of both description for a term which may also extend to 7 years, and shall additionally be vulnerable to fine.

- **Section 499 of the IPC:**

Any person who accepts that his/her notoriety is being hurt by an obvious portrayal distributed on the web can conjure this arrangement which solely represents comments via web-based networking media or indecent pictures or recordings posted for open utilization.

Under this arrangement, criticizing Women online will land the culprit in prison for a time of two years.

Section 411 of the IPC too prescribes punishment for dishonestly receiving stolen property and is worded in a way that is nearly equal to segment 66B of the IT Act. The punishment beneath phase 411 of the IPC is imprisonment of both descriptions for a time period of up to 3 years, or with best, or with each.

- **Section 503 of the IPC:**

On account of an individual compromising Women with the expectation to either alert her or insult her notoriety, the previous is obligated to be punished with a prison term of two years.

- **Section 507 of the IPC:**

Under this arrangement, any person who acts in light of a legitimate concern for scary or undermining a Women by unknown correspondence is at risk to be rebuffed with two years in jail.

- **Section509 of the IPC:**

Under this arrangement, individual particularly posting sexual/pictures/recordings involving sexual suggestions via web-based networking media is subject to three years of detainment alongside a fine against women.

Volume 10, May 2020 ISSN 2581-5504

AMENDMENTS TO THE IPC TO COVER CYBER CRIMES

The Indian legislature has from time to time, made a number of amendments to the IPC, to specially cowl cyber-crimes. Some of the crucial amendments are as follows:

- A brand new segment 29A was created to outline "electronic document" with the aid of linking it with the definition given within the IT Act;
- A new sub-section become inserted in phase four of the IPC (regarding the extension of the IPC to more territorial offences) that states that the provisions of the IPC shall be relevant to any man or woman in any vicinity "without and beyond India", committing an offence focused on a pc resource placed in India;
- In sections 118 and 119 of the IPC (that deal with the concealment of a design to commit an offence punishable with demise or imprisonment for existence and a public servant concealing a design to commit an offence which it's far his obligation to save you, respectively), the phrases "voluntarily conceals via any act or omission or by the usage of encryption or another statistics hiding device, the lifestyles of a design" had been inserted earlier than the phrases "to commit such offence or makes any illustration which he knows to be false respecting such design";
- In section 464 of the IPC (which penalises the making of a fake report), the word "digital signature" become replaced with the word "electronic signature" in all places. The section become also amended to encompass the making of fake digital records and affixing digital signatures below its ambit and the word "affixing electronic signature" changed into given the same that means as it has beneath the IT Act;
- "Electronic document" become included in the ambit of sections 164, 172, 173, one hundred seventy five, 192, 204, 463, 466, 468, 469, 470, 471, 474 and 476 of the IPC that earlier only furnished for "files", "books", "paper", "writing" or "records", as the case may be;
- In segment 466 of the IPC (which deals with forgery of courtroom statistics or of public registers), the term "sign up" became described to encompass any list, information or file of any entries maintained in an "electronic shape", as described in phase 2(1) (r) of the IT Act; and
- A new segment 354D became inserted within the IPC that introduces the offence of cyber stalking, which has been mentioned above.

Volume 10, May 2020 ISSN 2581-5504

CLASSIFICATION OF OFFENCES UNDER THE EXISTING INFORMATION TECHNOLOGY ACT, 2000

Under the existing IT Act, 2000, whether the offence under the IT Act is cognizable/bailable or otherwise was decided in accordance with Section 2 (a) & 2 (c) read with 1st Schedule of the Cr.P.C.,1973 because there was no specific provision under the existing IT Act, 2000 classifying the offences as cognizable/bailable or otherwise.

OFFENCE	**Cognizable or non-cognizable**	**Bailable or Non-bailable**
If punishable with death , imprisonment for life or imprisonment for more than 7 years	Cognizable	Non-Bailable
If punishable with imprisonment for 3 years and upwards but more than 7 years	Cognizable	Non-Bailable
If punishable with imprisonment for less than 3 years or with fine only	Non-Cognizable	Bailable

Thus, the offences under the existing IT Act, 2000 can be classified as follows:

Volume 10, May 2020 ISSN 2581-5504

SECTION & OFFENCE UNDER IT ACT,2000	**Punishment**	**Cognizable Or non-cognizable**	**Bailable or Non-bailable**
Section 65: Tampering with computer source documents	Imprisonment upto three years and/or Fine upto Rs. 2 Lakhs.	Cognizable	Non-bailable
Section 66: Hacking with Computer system	Imprisonment upto three years and/or Fine upto Rs. 2 Lakhs.	Cognizable	Non-bailable
Section 67: Publishing obscene information in electronic form	First Conviction: Imprisonment upto five years and Fine upto Rs.1 Lakh. . Second or subsequent Conviction: Imprisonment upto Ten years and Fine upto Rs. 2 Lakhs.	Cognizable	Non-bailable
Section 68 (2): Failure to comply with the order/direction of controller	Imprisonment for a term not exceeding three years or to a fine not exceeding two lakh rupees or to both.	Cognizable	Non-bailable

Volume 10, May 2020 ISSN 2581-5504

Section 69 (3): Failure to extend facilities to decrypt information to controller or any agency of government	Imprisonment for a term which may extend to seven years.	Cognizable	Non-bailable
Section 70 : Unauthorized access to protected system	Imprisonment up to 10 years and fine.	Cognizable	Non-bailable
Section 71: Penalty for misrepresentation	Imprisonment up to 2 years and/or fine upto Rs. 1 Lakhs.	Non-Cognizable	Bailable
Section 72: Breach of Confidentiality & privacy	Imprisonment up to 2 years and/or fine upto Rs. 1 Lakhs.	Non-Cognizable	Bailable
Section 73: Publishing false Digital Signature Certificate	Imprisonment up to 2 years and/or fine upto Rs. 1 Lakhs.	Non-Cognizable	Bailable
Section 74: Publication for fraudulent purpose	Imprisonment up to 2 years and/or fine upto Rs. 1 Lakhs.	Non-Cognizable	Bailable

Volume 10, May 2020 ISSN 2581-5504

CLASSIFICATION OF OFFENCES UNDER THE EXISTING INFORMATION TECHNOLOGY ACT, 2000 (AMENDMENT) BILL 2006

Section 77B was inserted in the bill of 2006.

Text -"S-77B Offences with three years imprisonment to be cognizable 1) Notwithstanding anything contained in Criminal Procedure Code 1973, the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable." The use of CrPC 1973 was made inapplicable.

OFFENCE	**Cognizable or Non- cognizable**	**Bailable or Non-bailable**
The offence punishable with imprisonment less than 3 years	Non-cognizable	Bailable
The offence punishable with imprisonment of three years	Cognizable	Bailable
The offence punishable with imprisonment of more than three years	Cognizable	Non-Bailable

The offences can be categorized as under:

Volume 10, May 2020 ISSN 2581-5504

SECTION & OFFENCES UNDER IT ACT 2000 AMENDMENT,2006	**Punishment**	**Cognizable or non-cognizable**	**Bailable or Non-bailable**
Section 65: Tampering with computer source documents	Imprisonment upto three years and/or Fine upto Rs. 2 Lakhs.	Cognizable	Bailable
Section 66: Hacking with Computer system (if done dishonestly or fraudulently)	Imprisonment upto three years and/or Fine upto Rs. 5 Lakhs.	Cognizable	Bailable
Section 66A: Punishment for sending offensive messages through communication service, etc	Imprisonment for a term which may extend to three years and with fine.	Cognizable	Bailable
Section 66B: Punishment for dishonestly receiving stolen computer resource or communication device	Imprisonment upto three years and/or Fine upto Rs. 1 Lakhs	Cognizable	Bailable
Section 66C: Punishment for identity	Imprisonment upto three years and Fine upto Rs. 1	Cognizable	Bailable

Volume 10, May 2020 ISSN 2581-5504

theft	Lakhs.		
Section 66D: Punishment for cheating by personation by using computer resource	Imprisonment upto three years and Fine upto Rs. 1 Lakhs.	Cognizable	Bailable
Section 66E: Punishment for violation of privacy	Imprisonment upto three years and/or Fine upto Rs. 2 Lakhs.	Cognizable	Bailable
Section 66F: Punishment for cyber terrorism	May extend to Life imprisonment.	Cognizable	Non bailable
Section 67: Publishing obscene information in electronic form	First Conviction: Imprisonment upto three years and Fine upto Rs. 5 Lakhs. Second or subsequent Conviction : Imprisonment upto five years and Fine upto Rs. 10 Lakhs.	Cognizable	Bailable in case of first conviction only. Second or subsequent conviction shall be non bailable
Section 67A: Punishment for publishing or transmitting of material containing sexually explicit act, etc. in	First Conviction: Imprisonment upto Five years and Fine upto Rs. 10 Lakhs Second or subsequent	Cognizable	Non-bailable in both first and second conviction

Volume 10, May 2020 ISSN 2581-5504

electronic form	Conviction : Imprisonment upto Seven years and Fine upto Rs. 10 Lakhs.		
Section 67B: Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form	First Conviction: Imprisonment upto Five years and Fine upto Rs. 10 Lakhs Second or subsequent Conviction : Imprisonment upto Seven years and Fine upto Rs. 10 Lakhs.	Cognizable	Non-bailable in both first and second conviction
Section 67C (2): Deliberate Failure by the intermediary to preserve and retain information as specified by the Central Government	Imprisonment upto three years and Fine	Cognizable	Bailable
Section 68 (2): Deliberate Failure to comply with the order/direction of controller	Imprisonment for a term not exceeding two years or to a fine not exceeding one lakh rupees or to both.	Non cognizable	Bailable
Section 69 (4): Failure to extend facilities to decrypt information to	Imprisonment for a term which may extend to seven years and fine.	Cognizable	Non bailable

Volume 10, May 2020 ISSN 2581-5504

govt. notified agency			
Section 69A (3): Punishment for failure by the intermediary to comply with the order of the notified agency to block websites etc.	Imprisonment for a term which may extend to seven years and fine.	Cognizable	Bailable
Section 69B (4): Deliberate failure by the intermediary to provide the notified agency with the technical assistance or online access to the computer resource	Imprisonment for a term which may extend to three years and fine.	Non Cognizable	bailable
Section 70: Unauthorized access to protected system directly or indirectly affects the facility of Critical Information Infrastructure	Imprisonment up to 10 years and fine.	Cognizable	Non bailable
Section 72A: Punishment for Disclosure of information in breach of lawful contract	Imprisonment for a term upto three years or to a fine upto Rs. 5 Lakhs or to both.	Cognizable	Bailable

Volume 10, May 2020 ISSN 2581-5504

16

CYBER FRAUDS IN INDIA

According to Norton Cybercrime Report 2012, 66% of Indian online adults have been a loss of computerized blackmail over an amazing span. In the past a year, 56% of online adults in India have experienced computerized distortion. As per the report, in any occasion 1,15,000 people fall prey to computerized coercion reliably, while 80 each second and more than one consistently provoking a climb in the typical direct budgetary cost per setback to around Rs10,500. According to the review, the cybercriminals have now moved their focus to the dynamically standard social stages. One out of three adults online Indians (32%) have been either social or adaptable cybercrime losses. While most web customers delete questionable messages and are mindful of their individual nuances on the web. In any case, 25% don't use complex passwords or change their passwords generally and 38% don't check for the lock picture in the program before entering sensitive individual information. Online adults are in like manner oblivious to the headway of most essential sorts of cybercrime. In all honesty, 68% of adults don't understand that malware can work in a reasonable structure, making it hard to tell whether a PC has been sabotaged, likewise, 33% (35%) don't know that their PC is starting at now great and liberated from contaminations.

HOW TO COMBAT CYBER CRIME

1. **DETECTION AND ANALYSIS**: To combat cybercrime it's important to know whether that head falls into the category of cybercrime or not. Once it is identified as a cyber-crime. We need to analyze whether it is cognizable or non- cognizable and bailable or non-bailable. It all depends upon the nature of crime. If we take an example of traditional crime like theft and rape. Both can't have same punishment, even though they both are crime. So we'll put theft under non-cognizable and bailable offence whereas rape will be considered as cognizable and non-bailable offence. In the same way if we take the case cyber copy right infringement it should fall in the category of cognizable and non-offence (with imprisonment of 3 years and fine depending upon the damage done to the injured party). Sale of illegal objects like drugs should also come under cognizable and non-bailable offence (with

[16] https://cyberpandit.org/?article_post=classification-of-offences-under-the-information-technology-law

REFERANCES:
1. http://cyberpolicebangalore.nic.in/pdf/Cyber%20law%20IPC.pdf
2. https://www.mondaq.com/india/it-and-internet/891738/cyber-crimes-under-the-ipc-and-it-act--an-uneasy-co-existence
3. https://shodhganga.inflibnet.ac.in/bitstream/10603/130487/8/08_chapter%202.pdf
4. https://shodhganga.inflibnet.ac.in/bitstream/10603/175612/9/09_chapter1.pdf
5. https://wcd.nic.in/sites/default/files/Protection%20of%20Children%20From%20Sexual%20Offences%20%28Amendment%29%20Act%2C%202019.pdf

Volume 10, May 2020 ISSN 2581-5504

imprisonment of more than 3 years and fine of Rs.10 lakh or more) .As selling of illegal articles can have bad impact on an individual or may be to a society to.

2. **PENALIZE**: Criminals should be punished (punishment can be in a form of imprisonment, fine or both) according to nature of crime. Law can't impose same punishment to a person who has committed cyber child pornography and other has committed an offence of cyber terrorism. Legislators before framing punishment for the offences and judges giving the judgement of an offence should first forecast to what extent injury and damage can occur whether it will effect only an individual or to large group of people.
3. **PREVENTION**:

A.EDUCATION AND CYBER SECURITY AWARENESS: This is one of the best digital security countermeasures, and a moment win.

- Teach workers to keep away from and forestall dubious movement on their PCs:
- Recognize dubious applications running, popups, cautioning messages, and so on.
- Banner dubious (messages with connections, sender obscure, hyperlinks and abnormal solicitations)
- Be watchful when perusing sites
- Stop and think before tapping on connections or advertisements
- Guarantee sites are dependable before entering qualifications
- Breaking point exercises when utilizing open uncertain Wi-Fi systems or utilize a VPN.

By instructing representatives on what to search for will expand the organization's capacity to perceive digital wrongdoing early and much of the time forestall digital wrongdoing. This ought to likewise be imparted and it won't just assistance the organization's digital cleanliness yet will enable the representative to keep their very own information secure.

Training judges and criminal lawyers and investigating and enforcement agencies to deal with this new transnational, complex, high-tech crimes to understand investigative and prosecution process that are unique to cybercrimes.

Preparing should begin at the highest point of the association, working down. It is prescribed to choose a digital security envoy inside every office to aid the identification and episode reaction for potential digital security dangers and dangers. This grows the productivity of any IT security group while guaranteeing that there is somebody in the association who is mindful and responsible for executing and keeping up digital safety efforts.

B. Keep frameworks and applications fixed and forward-thinking: Stay up with the latest and apply the most recent security fixes—this will keep most programmers and digital crooks from accessing frameworks by utilizing known adventures and vulnerabilities. This is anything

Volume 10, May 2020 ISSN 2581-5504

but a full verification counter measure; however it will make an effective break increasingly hard for digital lawbreakers.

C. Keep solid passwords and maintain special records: While picking a secret phrase make it a solid secret word, remarkable to that record, and change it regularly. The normal age of a social secret word today is years, and web based life doesn't work superbly cautioning you on how old your secret key is, the means by which frail it is, and when it is a decent an ideal opportunity to transform it. It is your obligation to secure your record along these lines, ensure it carefully. In the event that you have numerous records and passwords, utilize a venture secret key and special record vault to make it simpler to oversee and make sure about. Never utilize a similar secret phrase on different occasions.

D. Try not to permit clients to introduce or execute unapproved or untrusted applications – stop malware and ransomware at the endpoint: Another significant hazard that associations run—because of giving clients special access—is that the client can introduce and execute applications as they wish, regardless of where or how they acquired the establishment executable. This can represent a significant hazard permitting ransomware or malware to taint and proliferate into the association. Associations must actualize security controls that keep any application or instrument from being introduced onto the framework by utilizing Application Whitelisting, Boycotting, Dynamic Posting, Constant Benefit Rise, and Application Notoriety and Insight. This is one of the best approaches to forestall being the following survivor of digital wrongdoing.

E. Gather security logs and dissects for dubious or strange exercises: A significant movement and best practice for organizations is to ensure security logs are being gathered and investigated for dubious exercises. As a rule seeing security, logs will probably recognize anomalous activity. For instance, search for qualification logins or application executions that happened during non-business hours. Not exclusively can gathering security logs help recognize digital crimes, however they additionally become enormously significant when managing computerized legal sciences to decide underlying driver investigation and help with future counteraction measures.

4. LEGISLATION:

- Stricter laws should be made and enforced by legislation.
- A Special Bench for dealing with cybercrimes may be created at least in each and every High Court. Special branch may also be created in every metropolitan cities and districts.
- However The Indian Electronic Commerce Legislation has not addressed the following grey areas;
    A. Protection of domain name

Volume 10, May 2020 ISSN 2581-5504

B. Infringement of copy right laws
C. Jurisdiction aspect of electronic contracts
D. Taxation of goods and services traded through e-commerce
E. Stamp duty aspect of electronic aspect.

- Intellectual Property Laws still require major amendment to deal with challenges posed by the internet and digital revolution.
- There have been controversies to some act of IT which need to be modified. For example section 75 of the act.
- Stricter punishment should be imposed if regulation authorities appointed by the central government don't work properly.
- Some offences have been made compoundable which means parties can settle it between themselves because maximum cases target an individual. Sometimes it may be injustice for an individual as rich people can take advantage of this. They will start taking things for granted. For example making an MMS will be very normal for them.
- Narcotic Drugs and Psychotropic Substances (NDPS) Act, 1985, has not talked about online sale of illegal drugs.
- Certain limitations should be imposed on E- commerce.
- The legislation is required to pass laws like Economic Espionage Act for the protection of trade secrets, pragmatic steps is required to protect confidentiality of trade secrets during investigation and prosecution.
- More agencies should be made just like Computer Emergency Response Team (CERT).
- The amendments made by legislation ignore international classifications of cybercrimes. That should be added in an act.
- Special Statutes on cybercrime is required to be passed to deal with the new form of crimes and to protect digital data. It will include Intellectual Property crimes and crimes relating to human rights.
- The punishment for commission of cybercrimes to be increased to deter future offence. It must not only be deterrent but must also be exemplary.
- Better provisions should be made to secure electronic transaction, as our country is heading towards cashless economy.

CONCLUSION

Protections are expected to guarantee that laws that place limitations on Internet access and substance are not mishandled and are as per the standard of law and human rights. Lucidity in law is likewise expected to guarantee that laws are not used to disallow access to content in a way that abuses human rights law. A risk exists for "mission creep" or "capacity creep" (i.e., terms used to depict the development of law or potentially different measures in regions past

Volume 10, May 2020 ISSN 2581-5504

their unique degree), where laws and investigatory forces acquainted with target one type of cybercrime are then used to target other, less genuine types of cybercrime. Additionally, challenges concerning the compass and impact of cybercrime laws emerge where "Web content that is produced and adequate in one nation is made accessible in a third nation" where the substance is viewed as illicit. In spite of the fact that not all individuals are casualties to digital wrongdoings, they are still in danger. Violations by PC shift, and they don't generally happen behind the PC, yet they executed by computer. With the innovation expanding, lawbreakers don't need to ransack banks, nor do they need to be outside so as to carry out any wrongdoing.