# CYBER-CRIME: A THREAT TO DIGITAL ERA

Kaanchi Ahuja*


## *Abstract*

*Crime in a developing nation is viewed as a hindrance to its development as it adversely affects all members of the society, along with the security of the country. Technological advancements provided a necessary boost to efficiency and accuracy of human beings but at the same time it facilitated illegal use of digital technology for commission of cyber-crime. In today's world where everything is available at the option of a simple click, the possibility of committing a crime has also been made available at the instance of just a click. Cyber-Crime is an offence where the computer is either a tool or a target. The term WWW which stands for World Wide Web has now been replaced as World Wide Worry because of extensive growth and rapid increase in computer related crimes. The Government of India enacted a comprehensive statute called the Information Technology Act, 2000, while meticulously integrating international conventions, treaties and obligations. This Act covers the wide spectrum of technological information matters, which also including cyber violations, penalties and modes of curbing of cyber-crimes in India. This paper aims to identify the meaning of the term 'Cyber-crime' and enumerate the various types cyber-crimes committed in today's digital era. It also traces the development of cyber legislation in India and discusses the important case studies relating to matters concerning the cyber-crimes. Lastly, numerous positive remedies have also been incorporated for effectively curbing cyber-crimes in our country.*


***Keywords:*** *Cyber-crimes, IT Act, Cyber law legislation, Kinds of cyber-crime, Cyber Attacks*

* *Student-B.A.LL.B.(H)* @ Ideal Institute of Management and Technology, Affiliated to Guru Gobind Singh Indraprastha University, Delhi; Mobile: +91-9999344544; Email: kaanchiahuja1999@gmail.com

## INTRODUCTION

Crime is both a social and economic phenomenon. It is as old as human society. Plethora of prehistoric books and folklore stories have expressed and articulated different crimes committed either by individuals either against one another (civil crime) like theft or personal injury or crimes against the nation (criminal crime) like spying, treason or war. Our ancient Indian texts and scriptures, like the Kautilya's Arthashastra, which is written around 350 BC, is considered to be an authentic administrative treatise in India, which enumerates and explains in detail the various crimes and security protocol steps which were ought to be taken by the rulers against the possible happening of a crime in the state and also advocated punishment and compensation for a list of offences. Different kinds of punishments have been prescribed for listed offences and the concept of restoration of loss to the victims has also been discussed in it.

Crime in any form adversely affects all members of the society. Due to the huge perforation of technology in almost all walks of the society beginning from corporate governance and state administration and then commencing towards the small business and shop keepers who are computerizing their billing system, one can find computers and other electronic devices pervading the entire human life. Such is the power of digitisation and the penetration is so deep that a man cannot even spend a day without the electric devices.

The development and expansion of technology has made man rely on Internet for all his needs. Internet has given everyone an easy access to everything while sitting at their place of comfort. Social networking, online shopping, storing data, gaming, online studying, job search and online workplace transition, has resulted in man thinking that everything is easily possible in this digital era. The development of internet and its related benefit has also led to the origin, evolution and development of cyber-crimes. Cyber-crimes are committed on

plethora of platforms in diverse ways and because of lack of awareness; it could be carried out and committed very easily.

In matters of Cyber-Crime, India is also not far behind the other countries where the rate of incidence of cyber-crimes is increasing day by day. In a report published by the National Crime Record Bureau report (NCRB 2011) the incidence of cyber-crimes under the information Technology Act has increased by 85.4% in the year 2011 as compared to 2010 in India, whereas the increase in incidence of the crime under Indian Penal Code is by 18.5% as compared to the year 2010[1]. Vishakhapatnam has been marked with the maximum number of incidence of cases while Maharashtra has unfortunately developed into a centre of cyber-crimes with maximum number of incidence of registered cases under cyber-crimes category.[2] Hacking with computer systems and obscene publication were the main cases under the Information Technology Act for cyber-crimes. Maximum offenders arrested for cyber-crimes were in the age group of 18-30 years. 563 people in the age group of 18-30 years were arrested in the year 2010 which has increased to 883 in the year 2011.[3]

## GENESIS OF INFORMATION TECHNOLOGY LEGISLATION IN INDIA

The 1990s saw an advent growth in globalisation and computerisation with multiple nations computerising their governance and e-commerce witnessing an enormous spurt of growth. Until then, majority of the international trade and their transactions were facilitated and completed through documents which were transmitted either through post or by telex.

[1] The Hindu, '*NCRB data: Cyber-crimes reached a new high in 2017*', Available at: https://www.thehindu.com/data/cyber-crime-cases-in-india-jumped-77-in-2017-compared-to-2016/article29889061.ece ( Accessed on: August 02, 2020, 10:00 AM)

[2] DNA, '*Maharashtra leads in Cyber-Crimes*', Available at: https://www.dnaindia.com/india/report-maharashtra-leads-in-cyber-crimes-1709708 (Accessed on: August 02, 2020, 11:30 AM)

[3] National Crime Records Bureau, '*CHAPTER-18: CYBER-CRIMES*', Government of India, Available at: https://ncrb.gov.in/sites/default/files/crime_in_india_table_additional_table_chapter_reports/CHAP18_2003.pdf (Accessed on: August 02, 2020, 03:00 PM)

Evidences and records until then were majorly paper evidences and records with other forms of hard copies. Because bulk of international trade was carried out through electronic means and modes of communication, along with emailing system gaining momentum, an urgent and necessary need was felt for recognising electronic record i.e. the data what is stored in a computer and external storage.

The United Nations Commission on International Trade law (UNCITRAL) on E-commerce was adopted in 1996. The General Assembly of United Nations passed a resolution in January 1997 inter alia, recommending all the States in the United Nations to give favourable considerations to the said Model Law which provided for recognition of electronic records and treating it at par with paper documents (technological neutrality).

It is against this background that the Government of India enacted the Information Technology Act with the objective to provide legal recognition of transactions carried out by means of 'electronic commerce' which included the use of substitute communication and storage of information facility, to aid the process of electronic filing of documents with the Government agencies and further to amend the Indian Penal Code , the Indian Evidence Act , the Bankers Books Evidence Act and the Reserve Bank of India Act and for matters therewith or incidental thereto.

The Information Technology Act, 2000 was therefore passed as the Act No. 21 of 2000 and received the President assent on June 09 and was made effective from October 17, 2000.

The act recognises and accords the following issues:

1) Legal Recognition of Electronic Documents

2) Legal Recognition of Digital Signatures

3) Offenses and Contraventions

4) Justice Dispensation Systems for cyber-crimes

However, a need for an amendment – a detailed one – was felt for the Information Technology Act almost from the year 2003-2004. Numerous industry bodies were consulted for their expert assistance and advisory groups were organised to dwell into the perceived lacunae in the Information Technology Act for comparing it with similar legislations in other nations and thereby suggest recommendations.

Such recommendations were scrutinised and after consideration on such administrative plans, the consolidated Amendment Act (i.e. Information Technology Amendment Act 2008) and was placed before the Parliament of India. The Amendment Act 2008 got the President assent on February 05, 2009 and was made effective from October 27, 2009

**WHAT ARE CYBER-CRIMES?**

Cyber-crime is neither defined under Information Technology Act 2000 nor in the Information Technology Amendment Act 2008 nor in any legislation in India. In fact, the said terminology cannot be defined. Offence or crime has been dealt with elaborately listing various acts and the punishments for each under Indian Penal Code 1860, Code of Criminal Procedure 1908, Code of Criminal Procedure 1973 and quite a few other legislations too. Hence, to define cyber-crime, we can say in lay man understanding that it is just a combination of crime and computer. To further simply it, it can explained as 'any offence or crime in which a computer is used, is cyber-crime.'

Thought-provokingly enough, even a petty offence like stealing or pick-pocketing can be brought under the ambit and purview of cyber-crime if such data or aid has been utilised for committing such an offence and the same is facilitated by a computer or such information is stored in a computer and is used (or misused) by the fraudster. In a cyber-crime, computer or the data itself a target or manifests as the object of the offence or a tool in committing some

other offence, thereby providing the necessary inputs for that offence.

The Information Technology Act, 2000 defines various terminologies like computer, computer network, data, information and all other necessary pre-requisites that form part a cyber-crime. Cyber-crimes can be defined as unlawful acts wherein a computer is used as a tool or a target or combination of both. Cyber-crime is a general term that includes all types of digital crimes including credit card frauds, bank robbery, illegal downloading, industrial espionage, child pornography and denial of service attacks. It also covers crimes wherein computers or networks are used to enable and facilitate the desired illicit activity.

**TYPES OF CYBER-CRIME**

Cyber-crimes can be categorised in two ways:

1. The crimes in which the computer is targeted. Examples include hacking, virus attacks and DOS attacks.
2. The crimes in which the computer is used as a tool of weapon. Such crimes include cyber terrorism, intellectual property rights violations, credit card frauds, EFT frauds and pornography.

The different kinds of Cyber-Crimes can be categorised as:

1. *Unauthorised access and hacking*

Unauthorised access and hacking means any kind of access which is taken without the permission of the rightful owner or person in charge of the computer, computer system and computer network. Hacking means an illegal access into a computer system and/or network and every such act towards illegally entering into a computer and/or network is hacking. Hackers write or use computer programs and modules to attack the target computer. Majorly the act of hacking is committed for monetary gains, such as stealing the credit card

information, transferring money from various bank accounts to their own accounts followed by withdrawal of money. Government websites are the most targeted sites for the hackers. Recently the Indian Railway Catering and Tourism Corporation (IRCTC) the ticket-booking website of Indian Railways was hacked and the IRCTC officials fear that personal data including mobile numbers, credentials, personal information including date of birth and other important details of the customers have been sold for Rs. 15,000/- in a CD to the interested party.[4]

2. *Web hijacking*

Web hijacking means, taking forceful content of another person's website. In this case the owner of the website is deprived of the control over his website and its content.

3. *Pornography*

Pornography means showing sexual acts in order to because sexual excitement the definition of pornography also includes pornographic websites; pornographic magazines produced using computer and internet pornography delivered over mobile phones.

4. *Child Pornography*

The internet is being excessively used as a medium to sexually abuse children. The children are viable victim to the cyber-crimes. Computers and internet having become a necessity of every household, the children have got easy access to the internet. There is an easy access to the pornographic contents and paedophiles lure the children by distributing pornographic materials and then try to meet them for sex or take their nude photographs including their engagement in sexual acts and sexual positions.

[4] India Today, '*IRCTC website hacked, information of around 1 crore people feared stolen*', Available at: https://www.indiatoday.in/india/story/irctc-website-hacked-information-of-around-1-crore-feared-stolen-321712-2016-05-05 (August 03, 2020, 11:00 AM)

5. *Denial of Service Attack*

This is an act in which the hacker floods the bandwidth of the victim's network or fills his email box with spam mail depriving him of the services he is entitled to access. This is used to bring the network to crash by flooding it with useless traffic. Another variation to a typical denial of service attack is known as Distributed Denial of Service (DDoS) attack wherein the perpetrators are many and are geographically widespread. Many DoS attacks, such as Ping of Death and Teardrop attacks exploit limitations in the Intellectual Property protocols. For all types and kinds of DoS attacks, certain software's exist whereby system administrators can be installing to protect and limit the damage which might be caused by the attacks.

6. *Virus Attacks*

Viruses are the programs that have the capability to infect other programs and make copies of itself and spread into other programs programmes that multiply like viruses but spread from computer to computer are called worms. This software attaches them to other software. Virus, worms, Trojan horse, Time bomb, Logic Bomb, Rabbit and Bacterium are malicious viruses. Such viruses usually affect the data on a computer, either by altering or deleting it.

7. *Software Piracy*

Software piracy refers to illegal copying of programs or the counterfeiting and distribution of products. These kinds of crimes also include copyright infringement, trademark violations, computer source code theft and patent violations.

Domain names are also trademarks and protected by ICANN's domain dispute resolution policy and also under the trademark laws[5]. They register the domain name identical to

[5] World Intellectual Property Organisation (WIPO), '*WIPO Guide to the Uniform Domain Name Dispute Resolution Policy (UDRP)*', Available at: https://www.wipo.int/amc/en/domains/guide/ (August 03, 2020, 10 AM)

popular service provider's name so as to attract and defraud users[6].

*8. Salami attacks*

These attacks are used to instigate financial crimes. They key here is to make the alteration so insignificant that in a single case it would go completely unnoticed. For example, a bank employee inserting a program in the banking system which deducts a small amount of money (let's say Rs. 5/- a month) from the account of every customer. No account holder shall probably notice this unauthorised debit but the bank employee will make a considerable amount of money every month.

*9. Phishing*

It is an act of sending email to an entity or individual, falsely claiming to be an established, legitimate enterprise in order to scam the user into providing their private information which will be used for the purpose of identity theft. Such an email id or link or form would direct the user to visit the required website where they are asked to update personal information, such as passwords, credit card number, social security number and bank account details. The website however, in reality is a bogus site and is set up only for the purpose of stealing the user's information.

*10. Sale of illegal articles*

This category of cyber-crime includes the sale of narcotics, weapons and prohibited wildlife ornaments and skin by posting information on websites, auction sites and bulletin boards or simply by using email communication.

*11. Online gambling*

[6] Mondaq – Connecting knowledge and People, '*India: Cyber Squatting Laws In India*', Available at: https://www.mondaq.com/india/trademark/208840/cyber-squatting-laws-in-india (August 02, 2020, 04:00 PM)

There a million of websites, all hosted on servers abroad, that offer online gambling. It is believed that all these websites are actually frontiers for money laundering. Examples of Hawala transactions and money laundering with the help of digital platform over the internet have been reported.

*12. Email spoofing*

Email spoofying refers to email that appears to originate from one source but actually has been sent from another source. Emails spoofying can also cause monetary damage.

*13. Cyber defamation*

When a person publishes defamatory matter about someone on a website or sends emails containing defamatory information to all of the persons, friends it is termed as cyber defamation.

*14. Forgery*

Computers, printers and scanners are used to forge counterfeit currency notes, postage and revenue stamps, mark sheets etc. and are made with the help of computers, high quality printers or scanners.

*15. Theft of information contained in electronic form*

This cyber-crime category includes theft of information stored in computer hard disc, removable storage media etc.

*16. Email bombing*

This type of act refers to sending a numerous number of emails to a particular person so as to enable the email account (in case of an individual) or mail servers (in case of a company or an email service provider) to crash.

*17. 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 processing is completed. The dynamics of the information is changed from the way it should be entered into by inculcating a virus that changes data. This is done with the help of the programmer of the database or application, or anyone else involved in the process of having information stored in a computer file. It also involves automatic changing of the financial information for some time before processing and restoring the original information.

18. *Physically damaging a computer system*

As the name suggests, this type of offence involves theft of a computer, some part or parts of a computer or a peripheral attached to the computer.

*19. Breach or privacy or confidentiality*

Privacy is a fundamental and inherent right which is essential for protection of human dignity and security. Privacy enables us to produce and create barriers, which in turn helps us to manage boundaries which protect us from unwanted and unwarranted interference in our lives, therefore allowing us to determine who we are and how we want to interact with the world around us. Privacy enables us to establish boundaries and limitations for those who want to access our bodies, places, things, communication and information. Therefore breach of privacy can be understood as unauthorised use, distribution or disclosure of personal confidential information.

Confidentiality refers to protecting information from being accessed by unauthorised parties. In other words, only the people who are authorised to do so can gain access to sensitive data. A failure to maintain confidentiality means that someone who shouldn't have access has

managed to get it, through intentional behaviour or by accident. Such a failure of confidentiality, commonly known as breach, typically, cannot be remedied. Leakage of such information to other persons may cause damage to business or person and hence such information should be protected.

*20. E-commerce/ investment frauds*

Economic investment frauds are methods that use false and fake claims to impetrate investments, or sometimes call for the purchase, use or trade of forged or counterfeit securities. Such products and services which are purchased online or contracted by individuals digitally are in actuality, never delivered. This type of a fraud is a common example of misrepresentation of a product to entice customers for online transactions and non-delivery of products. Such fraudulent scheme makes and advertises a promise of exuberant high profits and gains.

**CYBER LAWS VIZ-A-VIS CYBER-CRIMES**

Numerous cyber offences have been made punishable under multifarious Indian Statutes. Some of these are as follows:

**I. Cyber-crime under Information Technology Act, 2000 ( Chapter XI)**

a. Section 65 deals with Tampering with Computer Source documents

b. Section 66 deals with Computer related Offences (Hacking in computer systems, Data alteration, etc.)

c. Section 66 A deals with Punishment for sending offensive messages through communication service, etc.

d. Section 66 B deals with Punishment for dishonestly receiving stolen computer

resource or communication device

e. Section 66 C deals with Punishment for identity theft

f. Section 66 D deals with Punishment for cheating by personation by using computer resource

g. Section 66 E deals with Punishment for violation of privacy

h. Section 66 F deals with Punishment for Cyber Terrorism

i. Section 67 deals with punishment for publishing or transmitting obscene material in electronic form

j. Section 70 deals with Protected Systems and authorisation in regard to this

k. Section 72 deals with Penalty for breach of confidentiality and privacy

l. Section 73 deals with Penalty for publishing [electronic signature] certificate false in certain particulars

**II. Cyber-crime under Indian Penal Code, 1860**

a. Section 383 deals with Extortion

b. Section 420 deals with Cheating and dishonesty inducing delivery of property

c. Section 463 deals with Forgery

d. Section 499 deals with Defamation

e. Section 500 deals with Punishment for Defamation

f. Section 503 deals with Criminal Intimidation

**III. Cyber-crime under Special Acts**

a. Online sale of drugs under Narcotic Drugs and Psychotropic Substances, 1985

b. Online sale of arms under the Arms Act, 1959

**COMBATING CYBER-CRIME UNDER INFORMATION TECHNOLOGY ACT, 2000**

The Information Technology Act totally has 13 chapters and 90 sections. The Act encompasses diverse headings commencing from definitions, authentication of electronic records, digital signatures, electronic signatures and much more. Elaborate procedures for certifying authorities (for digital certificates as per Information Technology Act 2000 and since replaced by electronic signatures in the Information Technology Amendment Act 2008) have also been spelt out.

The Information Technology Act 2000 defines many important words used in common computer parlances like Addressee[7], Affixing[8], Asymmetric Crypto System[9], Certificate Authority[10], Computer[11], Computer System[12], Communication Devices[13], Cyber Security[14], Digital Signature[15], Key Pair[16], Private Key[17] and Public Key[18].

Section 3 which was originally 'Digital Signature' was later renamed as 'Digital Signature and Electronic Signature' in the Information Technology Amendment Act 2008. Thus,

[7] Section 2(b), Information Technology Act, 2000

[8] Ibid, Section 2(d)

[9] Ibid, Section 2 (f)

[10] Ibid, Section 2(g)

[11] Ibid, Section 2(i)

[12] Ibid, Section 2(l)

[13] Ibid, Section 2(ha)

[14] Ibid, Section 2 (nb)

[15] Ibid, Section 2 (p)

[16] Ibid, Section 2(x)

[17] Ibid, Section 2 (zc)

[18] Ibid, Section 2(zd)

introducing technological neutrality by adopting electronic signatures as a legally valid for the purpose of executing signatures.

Section 4 to 10A deal with electronic governance issues and procedures and the legal recognition to electronic records. It discusses procedures on electronic records, storage, maintenance and validity of contracts formed through electronic means.

Procedures relating to electronic signatures and regulatory guidelines for certifying authorities have been laid down in the succeeding sections.

**IMPORTANT INDIAN CASE STUDIES**

1. *Nasscom* v. *Ajay Sood & Ors.*[19]

In a landmark judgement in the case of National Association of Software and Service Companies versus Ajay Sood and Others, the Delhi High Court declared 'phishing' on internet to be an illegal act, entailing an injunction and recovery of damages.

Explaining the concept of 'phishing' in order to provide a landmark precedent the court stated that it is a form of internet fraud where a person pretends to be a legitimate entity (like bank or insurance company) so as to extract personal information and data from a customer and gain unauthorised access to codes, passwords. Personal data so collected by misrepresenting the identity of legitimate party is commonly used for collecting an undue advantage. The Delhi High Court also stated that even though there is no specific legislation in India to penalise phishing, it held phishing to be an illegal act. Phishing was explained by the court as 'misrepresentation made in the course of trade leading to misunderstanding regarding the source and origin of e-mail. Such an act has the potential to cause extensive damage and loss not only to the customer but also to the person whose name, identity and password is

[19] 119 (2005) DLT 596, 2005 (30) PTC 437 Del

misused."

2. *Central Bureau of Investigation* v. *Arif Azim or SONY.SAMBANDH.COM CASE*[20]

India saw its first Cyber-Crime conviction in this case. A complaint was filed by Sony India Private Ltd, which runs a website called www.sony-sambandh.com which includes the participation of Non Resident Indians. It enables NRI's to send Sony products to their near and dear ones in India after they paying for it online though a digital portal and the company delivers these products to the recipients.

In May 2002, a person logged into this website and ordered a Sony Colour Television set and a cordless head phone. The person gave the credit card number for payment and requested that the products be delivered to Arif Azim in Noida. The payment was duly cleared and the company delivered the items to Arif Azim. However after 1.5 months the credit card agency informed the company that this was an unauthorized transaction as the real owner denied this purchase. The company lodged a complaint for online cheating with CBI. A case u/s 418, 419 and 420 of the IPC was filed and Arif Azim was arrested. Inquiry revealed that Arif Azim was working at a call centre in Noida and had gained unauthorised access to the credit card number of an NRI, which was further misused for this purchase. Arif pleaded guilty and the court convicted Arif Azim under Section 418, 419 and 420 of the Indian Penal Code.

3. *State (N.C.T. of Delhi)* v. *Navjot Sandhu @ Afsan Guru*[21](Parliament Attack Case)

Bureau of Police Research and Development (BRD), Hyderabad solved the complex task of retrieving information from the recovered laptop of terrorists who had planned and attacked Indian Parliament. The laptop was sent to Computer Forensics Division and the analysis proved that the laptop contained several evidences that confirmed of the two terrorists'

[20] 2003

[21] AIR 2005 SC 3820

motives, namely the sticker of the Ministry of Home that they had made on the laptop and pasted on their car to gain entry into Parliament House along with the fake ID card containing the Government of India emblem and seal.

4. *Shreya Singhal* v. *Union of India*[22]

Two women were arrested for posting allegedly offensive and objectionable comments on Facebook about the propriety of shutting down the city of Mumbai after the death of a political leader. The police arrest them under Section 66A of the Information Technology Act, 2000. However the police released the women and dismissed their prosecution. But such an incident invoked substantial criticism and these women then filed a petition, challenging the constitutional validity of Section 66A on the ground that it violates the right to freedom of expression. The Supreme Court declared Section 66A of the Information Technology Act, 2000 as unconstitutional and therefore declared it as null and void on grounds of violation of the freedom of speech guaranteed under Article 19(1) (a) of the Constitution of India and neither was it a 'reasonable restrictions' under Article 19(2).

5. First case convicted under Information Technology Act 2000 of India[23]

This case relates to obscene, defamatory and annoying message sent to a divorcee woman in the message group of Yahoo. The posting of the message resulted in humiliating and harassing phone calls to the lady in the belief that she was soliciting. Based on a complaint made in February 2004, the Police traced the accused to Mumbai and arrested him. The accused was a family friend of the woman and was allegedly interested in marrying her. She married another person but later divorce took place. The accused saw this as a new opportunity and started contacting her once again. On her reluctance to marry him, the

[22] (2013) 12 SCC 73

[23] *State of Tamil Nadu* v. *Suhas Katti*, CC No. 4680/2004

accused took up the harassment through the Internet. The Charge was filed under Section 67 of Information Technology Act 2000, 469 and 509 Indian Penal Code before the court. The court based came to the conclusion that the crime was conclusively proved. The court held that the origination of the obscene message was traced out and the real culprit was brought to the court. The accused was found guilty of offences under section 469, 509 IPC and 67 of IT Act 2000 and the accused is convicted and sentenced.

6. Two Nigerians sentenced seven years for online fraud[24]

A Kerala Court sentenced two Nigerians to five years rigorous imprisonment as they both had cheated a doctor in the Kerala district for Rs 30 lakh. The Nigerians were sentenced under sections 420, 468 of IPC and section 66(D) of Information Technology (Amendment) Act 2008. According to the case, the duo had cheated the doctor after they sent an e-mail asking to pay Rs 30 lakh as processing fee. A plan by the police succeeded when the Nigerians were lured into Kerala then arrested. This was the first verdict against financial fraud under the Information Technology Act.

## REMEDIES TO REDUCE COMPUTER RELATED OFFENCES

Multidimensional public or private or public-private collaborations between law enforcement agencies and information Technology & Information Security organisations can be established to handle the problem of cyber-crime. System consisting of software and hardware that authenticates both manual and automatic access and transfer of information should be regulated between organisations.

Some of the remedies which can be utilised to reduce computer related offences are enumerated as follows:

[24] Dhananjay, '*Cyber-Crime Convictions & Judgments*', Alert Indian, Available at: https://www.alertindian.com/node/18#gsc.tab=0 ( Accessed on: August 10, 2020, 11:00 AM)

1. Use different passwords and username combinations for forfeit accounts. One should update them every 6 months and should resist the urge to write them down somewhere,
2. Keep social media profiles like Facebook Twitter YouTube Snapchat LinkedIn private. Update the security settings frequently and be careful before agreeing to anything and staying alert when sharing any kind of information through your online posts,
3. Protect your sensitive data and information by using encryption method,
4. Do not share your personal identity credentials like name address phone number and financial information online,
5. Keep your computer current with the latest updates,
6. One of the best ways to keep cyber-crime and attackers away from one's computer is to administer software fixes and by regularly updating the computer from any incident of undue unauthorised advantage,
7. Protect your computer with security software. Security software includes firewall and antivirus programs which protect the computer's first line of defence. It protects communication and data stored in the computer and
8. When faced with such crimes, one should not panic but report the same to the local police. The following websites can provide help to any victim of cyber-crime:
    a. http://www.Cyber-Crimehelpline.com
    b. http://www.cyberpolicebangalore.nic.in
    c. http://www.cybercellmumbai.gov.in

## CONCLUSION

Since the advent of technological era and its development in the recent times, cyber-crimes has undertaken a disguised and distinguishing nature from the Internet and cyberspace and can be termed as invisible, technology - based crimes having no geographical borders. Cyber-crime investigation is not efficacious and fool proof as it has a high risk of failure due to misuse, stealing and destruction of evidence. There is a need to educate people and spread awareness about the consequences of cyber-crimes. There is also a need to regulate the social networking sites and its content flow. It should be mandatory for every citizen to adopt cyber etiquettes while utilising the online information and communication technology. The advent of technology within two decades has touched every individual life either directly or indirectly in this digital era, with its own advantages and disadvantages. Unfortunately so, it has also given birth to most deadly of crimes including cyber terrorism where a single click of a mouse can kill thousands of people. In order to legally control and prevent such crimes, the human kind needs to collectively be in pace with this technology and take informed decisions.