“Cybercrime” combines the term “crime” with the root “cyber” from the word “cybernetic”, from the Greek, “kubernan”, which means to lead or govern. The “cyber” environment includes all forms of digital activities, regardless of whether they are conducted through networks and without borders. This extends the previous term “computer crime” to encompass crimes committed using the Internet, all digital crimes, and crimes involving telecommunications networks. This more recent terminology covers a wide variety of facets, leading to different approaches, depending on the dominant culture of the experts, making it appear either reduced or expanded, in different dimensions, dealing with emerging issues that also reflect its diversity.

Cyber crime is one of the most common buzz words these days, the cases and the incidents of cybercrime sound insane sometimes cyber criminals show all their inhumanity by the cyber crimes they commit, before
we go on to know what is a cyber crime, we will know the meaning of a crime. Crime, in whatever forms it is, directly or indirectly, always affects the society. In today’s world, there is immense increase in the use of Internet in every field of the society and due to this increase in usage of Internet, a number of new crimes have evolved. Such crimes where use of computers coupled with the use of Internet is involved are broadly termed as Cyber Crimes.

These days’ computer and internet become very necessary and useful for our daily life. Today the internet is the great mediator of our lives. In present days people can get information, store information and share information through the internet. Back 20’s years later there was approx.100000 people uses internet but now around 3,405,518,376 people are surf the net around the globe. The growing fastest world of internet is known as cyber world. Today cyber world are fastest moving and high technology world. Asian countries are most uses of internet in the world. In Asia region India has rank top two internet users country, so India is the very fastest growing country. Today internet becomes the backbone of social & economic world. Users can access the internet anytime from anywhere but through the internet many illegal works may done. Today E-mail and website is the most efficient way of data communication. Cyber crimes are technology based crimes and the computer or internet itself can be used as a weapon or means to do such crimes quite freely. They are organized and white collar crimes like cyber frauds, hacking, data theft, phishing, identity theft etc. Cyber crimes are committed with the help of technology and cyber criminals have deep understanding of technology. In fact, cyber criminals are technocrats who understand the intricacies of information technology. Cybercrimes do not consider any boundaries or territorial barriers.

According to Information Technology Act, 2000 Cyber Crime is “the acts that are punishable by the Information Technology Act”. It is not exhaustive as the Indian Penal Code also covers many cyber crimes, such as email spoofing and cyber defamation, sending, threatening emails. This work seeks to define the concept of cyber-crime, identify reasons for cyber-crime, how it can be eradicated, look at those involved and the reasons for their involvement, we would look at how best to detect a criminal mail and in conclusion, proffer recommendations that would help in checking the increasing rate of cyber-crimes and criminals.

History of cybercrime:
The first recorded cyber crime took place in the year 1820. In 1820, Joseph Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard’s employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This is the first record of cyber crime.

Cyber crime meaning:
Cyber-crime by definition is any harmful act committed from or against a computer or network, it differs according to McConnell International, “from most terrestrial crimes in four ways: they are easy to learn how to commit, they require few resources relative to the potential damages caused, they can be committed in a jurisdiction without being physically present in it and fourthly, they are often not clearly illegal.” Another definition given by the Director of Computer Crime Research Centre (CCRC) during an interview on the 27th April, 2004, is that “cyber-crime (‘computer crime’) is any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them.” In essence, cyber-crime is crime committed in a virtual space and a virtual space is fashioned in a way that information about persons, objects, facts, events, phenomena or processes are represented in mathematical, symbol or any other way and transferred through local and global networks.

From the above, we can deduce that cyber crime has to do with wrecking of havoc on computer data or networks through interception, interference or destruction of such data or systems. It involves committing crime against computer systems or the use of the computer in committing crimes.

Types of cyber attack:
Hacker: hacker is an unauthorized user who attempts to or gains access to an information system. Hacking is
a crime even if there is no visible damage to the system, since it is an invasion in to the privacy of data.

E-mail spoofing and E-mail bombing: A spoofed email is one that appears to originate from one source but actually has been sent from another source. This can also be termed as E-Mail forging. In this case, the goal of the attacker is to interrupt the victim’s e-mail service by sending him a large number of emails.

Domain hijacking: It is the act of changing the registration of a domain name without the permission of its original registrant.

Software piracy: Many people do not consider software piracy to be theft. They would never steal a rupee from someone but would not think twice before using pirated software. There is a common perception amongst normal computer users to not consider software as property. This has led to software piracy becoming a flourishing business. The software pirate sells the pirated software in physical media usually CD ROM through a close network of dealers.

Cyber pornography:
This would include pornographic websites; pornographic magazines produced using computers (to publish and print the material) and the Internet (to download and transmit pornographic pictures, photos, writings etc). Recent Indian incidents revolving around cyber pornography include the Air Force Balbharati School case. A student of the Air Force Balbharati School, Delhi, was teased by all his classmates for having a pockmarked face. Tired of the cruel jokes, he decided to get back at his tormentors. He scanned photographs of his classmates and teachers, morphed them with nude photographs and put them up on a website that he uploaded on to a free web hosting service. It was only after the father of one of the class girls featured on the website objected and lodged a complaint with the police that any action was taken. In another incident, in Mumbai a Swiss couple would gather slum children and then would force them to appear for obscene photographs. They would then upload these photographs to websites specially designed for pedophiles. The Mumbai police arrested the couple for pornography.

Identity theft: It simply refers to fraud or cheat others by make their wrong identity of others. It involves stealing money or getting other benefits by pretending to someone else Information Technology (Amendment)Act, 2008, crime of identity theft under Section 66-C.Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, known as identity theft For which criminal shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Cyber crime cases in India:
Pune Citibank Emphasis call center fraud:
It is a case of sourcing engineering. US $ 3, 50,000 from City bank accounts of four US customers were dishonestly transferred to bogus accounts in Pune, through internet. Some employees of a call centre gained the confidence of the US customers and obtained their PIN numbers under the guise of helping the customers out of difficult situations. Later they used these numbers to commit fraud. Highest security prevails in the call centers in India as they know that they will lose their business. The call center employees are checked when they go in and out so they cannot copy down numbers and therefore they could not have noted these down. They must have remembered these numbers, gone out immediately to a cyber café and accessed the Citibank accounts of the customers. All accounts were opened in Pune and the customers complained that the money from their accounts was transferred to Pune accounts and that’s how the criminals were traced. Police has been able to prove the honesty of the call center and has frozen the accounts where the money was transferred.

Andhra Pradesh tax case:
The owner of a plastics firm in Andhra Pradesh was arrested and Rs. 22 crore cash was recovered from his house by the Vigilance Department. They sought an explanation from him regarding the unaccounted cash. The accused person submitted 6,000 vouchers to prove the legitimacy of trade, but after careful scrutiny of vouchers and contents of his computers it revealed that all of them were made after the raids were conducted. It was revealed that the accused was running five businesses under the guise of one company and used fake and computerized vouchers to show sales records and save tax. Thus the dubious tactics of the prominent businessman from Andhra Pradesh was exposed after officials of the department got hold of
computers used by the accused person.

Parliament attack case:
Bureau of Police Research and Development at Hyderabad had handled some of the top cyber cases, including analyzing and retrieving information from the laptop recovered from terrorist, who attacked Parliament. The laptop which was seized from the two terrorists, who were gunned down when Parliament was under siege on December 13 2001, was sent to Computer Forensics Division of BPRD. The laptop contained several evidences that confirmed of the two terrorists’ motives, namely the sticker of the Ministry of Home that they had made on the laptop and pasted on their ambassador car to gain entry into Parliament House and the fake ID card that one of the two terrorists was carrying with a Government of India emblem and seal. The emblems (of the three lions) were carefully scanned and the seal was also crafty made along with residential address of Jammu and Kashmir. But careful detection proved that it was all forged and made on the laptop.

The bank NSP case:
The Bank NSP case is the one where a management trainee of the bank was engaged to be married. The couple exchanged many emails using the company computers. After some time the two broke up and the girl created fraudulent email ids such as “Indian bar associations” and sent emails to the boy’s foreign clients. She used the banks computer to do this. The boy’s company lost a large number of clients and took the bank to court. The bank was held liable for the emails sent using the bank’s system.

Present trends of Cybercrime in India:
India is trying to implement the Digital India project to the best of its capabilities. The success of Digital India project would depend upon maximum connectivity with minimum cyber security risks. This is also a problem for India as India has a poor track record of cyber security. According to Home Ministry statistics, as many as 71,780 cyber frauds were reported in 2013, while 22,060 such cases were reported in 2012. There have been 62,189 incidents of cyber frauds till June 2014. In 2013, a total of 28,481 Indian websites were hacked by various hacker groups spread across the globe. The numbers of hacking incidents were 27,605 in 2012 and 21,699 in 2011. As per the cyber-crime data maintained by National Cyber Records Bureau, a total of 1,791, 2,876 and 4,356 cases were registered under the Information Technology Act in 2011, 2012 and 2013, respectively. A total of 422, 601 and 1,337 cases were registered under cyber-crime related sections of the Indian Penal Code in 2011, 2012 and 2013, respectively. There has been an annual increase of more than 40 per cent in cyber-crime cases registered in the country during the past two-three years.

Causes for cyber crime:
There are many reasons why cyber-criminals commit cyber-crime, chief among them are these three listed below:
Cyber crimes can be committed for the sake of recognition. This is basically committed by youngsters who want to be noticed and feel among the group of the big and tough guys in the society. They do not mean to hurt anyone in particular; they fall into the category of the Idealists; who just want to be in spotlight.
Another cause of cyber-crime is to make quick money. This group is greed motivated and is career criminals, who tamper with data on the net or system especially, e-commerce, e-banking data information with the sole aim of committing fraud and swindling money off unsuspecting customers.
Thirdly, cyber-crime can be committed to fight a cause one thinks he believes in; to cause threat and most often damages that affect the recipients adversely. This is the most dangerous of all the causes of cyber-crime. Those involve believe that they are fighting a just cause and so do not mind who or what they destroy in their quest to get their goals achieved. These are the cyber-terrorists.

Definition of Cybercrime:
Defining cyber crimes, as “acts that are punishable by the Information Technology Act” would be unsuitable as the Indian Penal Code also covers many cyber crimes, such as email spoofing and cyber defamation,
sending threatening emails etc. A simple yet sturdy definition of cyber crime would be “unlawful acts wherein the computer is either a tool or a target or both”.

At the onset, let us satisfactorily define “cyber crime” and differentiate it from “conventional Crime”. Computer crime can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000. Defining cyber crimes, as “acts that are punishable by the Information Technology Act” would be unsuitable as the Indian Penal Code also covers many cyber crimes, such as email spoofing and cyber defamation, sending threatening emails etc.

Simple yet sturdy definition of cyber crime would be “unlawful acts wherein the computer is either a tool or a target or both”. Let us examine the acts wherein the computer is a tool for an unlawful act. This kind of activity usually involves a modification of a conventional crime by using computers.

Aspects of Cyber crime:

Technological Aspect of Cybercrime:
From a technological dimension, other experts point out the need for a comprehensive term, such as “electronic crime” or “e-crime”, thanks to the convergence of ICT, including mobile technology, telephony, memory, surveillance systems, and other technologies, including nanotechnology and robotics, which must be taken into account from now on. These electronic media will be targeted increasingly more often and will also be used to conceal, commit, or support crimes and offenses. Only the positive actions for which one or more means were used to commit one of the elements of the offense can be included.

Anthropological Aspect of Cybercrime:
From an anthropological aspect, cybercrime originates from various populations and exhibits socio-educational, socio-economic, and techno-ideological factors and their expressions, including pathological expressions like addiction. The maladjustment of the education system may contribute to the development of new forms of cybercrime or deviant practices and behavior with various levels of severity, including cheating and reputational damage, which can be related to frustrations and the redefinition of material and citizen values, inconsistent with what is expected when approaching and leading an adult life. Difficult socio-economic conditions also include the Internet as a place for expressing psychological troubles with socio-economic origins, including theft, child pornography, and calls for uprisings, violence, and hatred. With regard to techno-ideological factors, one must consider sites and networks aimed at propaganda, destabilization, and individual and mass psychological manipulation using methods that involve the digital processing of images, videos, and audio.

Strategic Aspect of Cybercrime:
From a strategic aspect, cybercrime is seen as an offense to cyber-security, namely attacks to digital networks for the purpose of seizing control, paralyzing them, or even destroying infrastructures that are vital to governments and sectors of vital importance.

Objectives:
To examine the awareness of cyber crime.
To understand individuals knowledge about cyber crime.
To analyze the principles of jurisdiction in cyber offences.

Importance:
Cyber crime is an intangible dimension that is impossible to govern and regulate using conventional law.
Cyber crime handles gigantic traffic volumes every second.
It offers never seen before economic efficiency.
Electronic information has become the main object of cyber crime

Scope of the study:
To identify the drawbacks of cyber law in India.
To improve cyber law system in India.
Creating awareness about cyber crime among the people.
In near future cyber law has great scope in the corporate world.

CHAPTER 2
RESEARCH STUDY

CHAPTER 2
RESEARCH STUDY
Title of the study:
Cyber Crime in India

Statement of the problem:
Rapid developing of telecommunication and global computer network has created the reasons, which allow to commit cyber crimes in the highly technologies field. Day by day cyber crime is increasing in India. Since 2015 cyber crime has been increased by 300% in India. The ‘Internet’ has given many gifts to humanity but they come with unexpected pitfalls. It has become a place to do all sort of activities which are prohibited by law. It is increasingly being used for pornography, gambling, trafficking in human organs and prohibited drugs, hacking, infringing copyright, terrorism, violating individual privacy, money laundering, fraud and software piracy etc. Cyber crime is not only a matter of concern for India but it is also a global problem and therefore the world at large has to come forward to stop cyber crime.

Review of literature:
Justice Yatindra Singh in his book “Cyber Laws”9 has elaborately discussed the meaning and importance of intellectual property rights like trademarks, copyrights, patents etc. vis-à-vis cyber space. According to him, these rights refer to the property that is a creation of the mind i.e. inventions, literary and artistic works, symbols, names, images, and designs used in commerce.10 As far as the infringement of IPRs in cyberspace is concerned he has critically analyzed the judgments of Napster Case,11 Sony Play Station Case12 and Grokster Case.
Vivek Sood in his book “Cyber Crimes, Electronic Evidence and Investigation: Legal Issues”14 has suggested various strategies to curb cyber crimes. He says that since cyber crimes are technology based, so the best answer to these crimes is security technology.15 Fire-walls, anti-virus software and anti-intrusion systems are some of the effectively used security technologies. He concluded that “protect yourself” is the best mantra against cyber crimes.16 According to him, effective cooperation between the law enforcement agencies within the country and between nations is also necessary to challenge cyber criminals and bring them before the law. Further he calls for strengthening of extradition treaties and their implementation as a must in this digital age.
Dr. Vishwanath Paranjape in his book “Legal Dimensions of Cyber Crimes and Preventive Laws with Special Reference to India”17 has pointed out that with the rapid development of computer technology and internet over the years, the problem of cyber crime has assumed gigantic proportions and emerged as a global issue.18 He has suggested the need for international cooperation to combat cyber crimes and in this regard he has comprehensively discussed various national and international conventions, conferences, summits etc. relating to cyber crimes along with the municipal cyber legislations of different countries like UK, USA, India, Canada, China, Japan, Germany, Australia, and France etc.
Nandan Kamath in his book “Law relating to Computers, Internet and E-commerce: A Guide to Cyber Laws and the Information Technology Act, 2000”19 has commented on the emerging field of ‘electronic evidence’ in the cases of cyber crimes. He has made an in-depth study about the admissibility and authenticity of electronic records, burden of proof in cyber offences, and of certain other concepts like production and effect of such evidences, video-conferencing, forensic computing and best evidence rule etc.
Ahmad, Farooq in his article “Interplay of Internet Domain Names and Trademark Law” has observed that internet domain names have spawned unprecedented legal issues which do not have express solution. Though the courts have accorded equal protection to trademarks and domain names, but still domain names
are at stake due to highly technical nature of computers and internet. He has given a detailed account of the role of Uniform Domain Name Dispute Resolution Policy (UDRP) in protecting domain names. S.K. Verma and Raman Mittal in their book "Legal Dimensions of Cyber Space" have explained the basic concepts of cyber world like meaning, types, features and major components of computers; history and development of internet; merits and limitations of internet; various computer contaminants like virus, worms, Trojans etc. Emphasizing on the importance of computers and internet in day-to-day chores they have opined that "today it touches and influences almost every aspect of our lives. We are in the information age and computers are the driving force. We hardly do any activity that is not in some way dependent on computers." They further suggest that not only do we need to be computer-literate, but we also need to understand the myriad issues that surround our extensive and necessary dependence on computers. Commenting on the interlink of human-conflicts-law, they states that where humans are, crime and conflict of interests cannot be far behind, further, where crime and conflict of interests are, law must necessarily march in order to take control and regulate. Thus, they have made a detailed study on the indispensable role of computer and internet, and the resultant cyber crimes.

Vakul Sharma in his book "Information Technology; Law and Practice" has evaluated the issue of jurisdiction in cyber space. While discussing the role of international law in deciding jurisdiction of cyber offences he has made references to various principles like territorial principle, nationality principle, protective principle, passive personality principle, effects principle and universality principle. Further, he has made deep insight into the controversial issue regarding extradition of cyber criminals. Moreover, he has examined the US, European and Indian approaches towards personal jurisdiction at a greater length. V.D. Dudeja in his book "Cyber Crime and the Law" has highlighted the interplay of freedom of expression and the internet. Enumerating the reasonable restrictions on the freedom of expression he has concluded that in the interests of privacy and security some restrictions can also be put on the use of computers and internet because law has been able to recognize computer as a 'weapon of offence' as well as a 'victim of crime' leading to the emergence of cyber jurisprudence.

Sampling:
Survey is made among students and employed people.
Survey is conducted among 50 people.
Targeted population are students and employees.
Random sampling method is done because the population is finite.

Methodology:
The primary data is collected with the help of questionnaire from the customers in the city of Bangalore. Survey of students and employed are done.
Primary data are been taken to collect survey.
Survey data have been collected through online bases, through "Google Forms".
The secondary data is collected through Online and desk based reviews of books, journals, reports, research articles, and magazines.

Limitation of the study:
Study is only limited to students and employee.
Due to time consistent the study is made only among 50 respondents.
Primary data has been used to collect survey.
Survey has conducted among students and employed.
Survey has been conducted within our locality.

Chapter Scheme:

CHAPTER TOPICS

CHAPTER 1:-INTRODUCTION
Brief introduction
History of cyber crime
Meaning
Types of attack
Cyber crime cases in India
Present trends of cyber crime
Causes for cyber crime
Definition
Aspects
Objectives
Importance
Scope if the study

CHAPTER 2:- RESEARCH STUDY
Title of the study
Statement of the problem
Review of literature
Sampling
Methodology
Limitation of study
Chapter scheme

CHAPTER 3:- DATA ANALYSIS AND INTERPRETATION
Title of project
Data Table
Analysis of the table
Graphical representation

CHAPTER 4:- FINDINGS, CONCLUSIONS AND RECOMMENDATIONS.
Findings
Recommendations
Conclusion

APPENDICES AND ANNEXURE

Questionnaire

BIBLIOGRAPHY

References
Websites

About Essay Sauce

EssaySauce.com is a completely free resource to help students research their academic work and learn from great essays!

View all posts by Essay Sauce

...(download the rest of the essay above)
About EssaySauce, the student essay site:

EssaySauce.com is a free resource for students, providing thousands of example essays to help them complete their college and university coursework. Students can use our free essays as examples to write their own.

Latest student essays:

DON DRAPER’S ELECTRIC DREAMS
Enhancing SLCN learning in SEND children through music intervention
The White Tiger – Aravind Adiga
Symbolism in William Golding’s Lord of the Flies
Beowulf – Heaney
The tort of negligence / standard of care
The law of nuisance
Imprisonment in Ireland
Adam’s Curse – Yeats
Student essay categories:

Accounting essays
Architecture essays
Business essays
Computer science essays
Criminology essays
Economics essays
Education essays
Engineering essays
English language essays
English literature essays
Environmental studies essays
Finance essays
Geography essays
Health essays
History essays
Hospitality and tourism essays
Human rights essays
Information technology essays
International Relations
Law essays
Leadership essays
Linguistics essays
Literature essays
Management essays
Marketing essays
Media essays
Medicine essays
Miscellaneous essays
Music Essays
Philosophy essays
Photography and arts essays
Politics essays
Project management essays
Psychology essays
Religious studies and Theology essays
Science essays
Social work essays
Average review:

Overall rating: 0 out of 5 based on 0 reviews.

Q: Is EssaySauce.com free?

Yes! EssaySauce.com is a completely free resource for students. You can view our terms of use here.

Why use Essay Sauce?

The brightest students know that the best way to learn is by example! EssaySauce.com has thousands of great essay examples for students to use as inspiration when writing their own essays.

Is Essay Sauce completely free?

Yes! EssaySauce.com is a completely free resource for students. You can view our terms of use here.

Footer Widget

Replace this widget content by going to Appearance / Widgets and dragging widgets into this widget area.

To remove or choose the number of footer widgets, go to Appearance / Customize / Layout / Footer Widgets.