VOLUME 2 | ISSUE 1 | ISSN 2456-9704

AN OVERVIEW OF CYBER CRIME AND CYBER SECURITY

By: Shivapriya . K
Assist Professor', Sri Kengal Hanumanthaiya Law College,

ABSTRACT

In the era of cyber world as the usage of computers became more popular, there was expansion in the growth of technology as well, and the term 'Cyberspace particularly cyber space.'is used as platforms int the communication of information and the delivery of services. Cyber law is aterm used to describe the legal issue related to use of communication, technology became more familiar to the people. The evolution of Information Technology (IT) gave birth to the cyber space wherein internet provides equal opportunities to all the people to access any information, data storage, analyse etc. with the use of high technology. Due to increase in the number of netizens, misuse of technology in the cyberspace was clutching up which gave birth to cyber crimes at the domestic and international level as well.

Though the word Crime carries its general meaning as "a legal wrong that can be followed by criminal proceedings which may result into punishment" whereas Cyber Crime may be "unlawful acts wherein the computer is either a tool or target or both".

Cyber crimes also includes criminal activities done with the use of computers which further perpetuates crimes i.e. financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail, spoofing, forgery, cyber defamation, cyber stalking, unauthorized access to Computer system, theft of information contained in the electronic form, e-mail bombing, physically damaging the computer system etc.

Cyber security is necessary since it helps in securing data from threats such as theft or misuse, also safeguards your system from viruses.

Major Security Problems : Virus, Hacker, Malware, Trojan horses, Password Cracking

Safety tips to Cyber Crime :
Use antivirus software, Insert Firewalls, Uninstall unnecessary software, Maintain backup, Check security settings, **Stay anonymous :** Choose a genderless screen name never give your name or address to strangers.

Introduction :

Crimes by computer vary and they don't always occur behind the computer, but they executed by computer though all people are not victims to cyber crime but still there are in risk of hesitation in using the computer and internet. With increase in technology the criminals don't have to rob banks, nor do they have to be outside in order to commit any crime. They have everything they need or their lap. Their weapons are not guns anymore, they attack with mouse, cursers and passwords.

Meaning of cyber crime :

VOLUME 2 | ISSUE 1 | ISSN 2456-9704

The crime committed using a computer and the internet to steal a person's identity. Cyber Crime or computer related crime, is crime that involves a computer and a network. The computer may have been used in the commission it may be a target of crime, or cyber crime may threaten a person or a nation security and financial health.

The Cyber Crime committed using a computer and the internet to steal a person's identity or illegal imports. The first recorded cyber crime took place in the year 1820.

Categories of Cyber Crime :

- Computer as a target : Using a computer to attacks other computer. eg. hacking, virus forms attacks.
- Computer as a weapon : Using a computer to commit real world crime.
  eg. Cyber terrorism, credit card fraud and pornography etc.

Classification of Cyber Crime :

Cyber Crimes which are growing day by day, it is very difficult to find out what is actually a cyber crime and what is the conventional crime so to come out of this confusion, cyber crimes can be classified under different categories which are as follows:

- Cyber Crime Against Person
- Cyber Crimes Against Persons Property
- Cyber Crimes Against Government
- Cyber Crimes Against Society at large

1. **Cyber Crimes against Persons:**

There are certain offences which affects the personality of individuals can be defined as:

- **Harassment via E-Mails:** It is very common type of harassment through sending letters, attachments of files & folders i.e. via e-mails. At present harassment is common as usage of social sites i.e. Facebook, Twitter etc. increasing day by day.
- **Cyber-Stalking:** It means expressed or implied a physical threat that creates fear through the use to computer technology such as internet, e-mail, phones, text messages, webcam, websites or videos. Cyber stalking involves use of internet to harasse some one. The behaviour includes normally majority of Cyber Stalkers are men and majority of victims of women.
- **Dissemination of Obscene Material:** It includes Indecent exposure/ Pornography (basically child pornography), hosting of web site containing these prohibited materials. These obscene matters may cause harm to the mind of the adolescent and tend to deprave or corrupt their mind.
- **Defamation:** It is an act of imputing any person with intent to lower down the dignity of the person by hacking his mail account and sending some mails with using vulgar language to unknown persons mail account.
- **Hacking:** It means unauthorized control/access over computer system and act of hacking completely

VOLUME 2 | ISSUE 1 | ISSN 2456-9704

destroys the whole data as well as computer programmes. Hackers usually hacks telecommunication and mobile network.

- **Cracking:** It is amongst the gravest cyber crimes known till date. It is a dreadful feeling to know that a stranger has broken into your computer systems without your knowledge and consent and has tampered with precious confidential data and information.
- **Spoofing :** It is the act of disguising one computer to electronically "look" like another computer, in order to gain access to a system that would be normally restricted.
- **E-Mail Spoofing:** A spoofed e-mail may be said to be one, which misrepresents its origin. It shows it's origin to be different from which actually it originates.
- **SMS Spoofing:** Spoofing is a blocking through spam which means the unwanted uninvited messages. Here a offender steals identity of another in the form of mobile phone number and sending SMS via internet and receiver gets the SMS from the mobile phone number of the victim. It is very serious cyber crime against any individual.
- **Carding:** It means false ATM cards i.e. Debit and Credit cards used by criminals for their monetary benefits through withdrawing money from the victim's bank account mala-fidely. There is always unauthorized use of ATM cards in this type of cyber crimes.
- **Page Jacking :** When a user, click on a certain link and an unaccepted web site gets opened through that link, someone steals apart of real website and uses it in a fake site.
- **Cheating & Fraud:** It means the person who is doing the act of cyber crime i.e. stealing password and data storage has done it with having guilty mind which leads to fraud and cheating.
- **Child Pornography:** It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children.
- **Assault by Threat:** refers to threatening a person with fear for their lives or lives of their families through the use of a computer network i.e. E-mail, videos or phones.

2. Crimes against Persons Property:

As there is rapid growth in the international trade where businesses and consumers are increasingly using computers to create, transmit and to store information in the electronic form instead of traditional paper documents. There are certain offences which affects persons property which are as follows:

- **Intellectual Property Crimes:** Intellectual property consists of a bundle of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an offence. The common form of IPR violation may be said to be

VOLUME 2 | ISSUE 1 | ISSN 2456-9704

software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc .

- **Cyber Squatting:** It means where two persons claim for the same Domain Name either by claiming that they had registered the name first on by right of using it before the other or using something similar to that previously. For example two similar names i.e. www.yahoo.com and www.yaahoo.com.
- **Cyber Vandalism:** Vandalism means deliberately destroying or damaging property of another. Thus cyber vandalism means destroying or damaging the data when a network service is stopped or disrupted. It may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer.
- **Corporate Espionage :** Means theft of trade secrets to illegal means such as wire taps or illegal intrusions.
- **Hacking Computer System:** Hacktivism attacks those included Famous Twitter, blogging platform by unauthorized access/control over the computer. Due to the hacking activity there will be loss of data as well as computer. Also research especially indicates that those attacks were not mainly intended for financial gain too and to diminish the reputation of particular person or company.
- **Transmitting 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 usually affect the data on a computer, either by altering or deleting it. Worm attacks plays major role in affecting the computerize system of the individuals.
- **Cyber Trespass:** It means to access someone's computer without the right authorization of the owner and does not disturb, alter, misuse, or damage data or system by using wireless internet connection.
- **Internet Time Thefts:** Basically, Internet time theft comes under hacking. It is the use by an unauthorised person, of the Internet hours paid for by another person. The person who gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge. You can identify time theft if your Internet time has to be recharged often, despite infrequent usage.

3. **Cybercrimes Against Government:**

There are certain offences done by group of persons intending to threaten the international governments by using internet facilities. It includes:

- **Cyber Terrorism:** Cyber terrorism is a major burning issue in the

VOLUME 2 | ISSUE 1 | ISSN 2456-9704

domestic as well as global concern. The common form of these terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate e-mails, attacks on sensitive computer networks etc. Cyber terrorism activities endanger the sovereignty and integrity of the nation.

- **Cyber Warfare:** It refers to politically motivated hacking to conduct sabotage and espionage. It is a form of information warfare sometimes seen as analogous to conventional warfare although this analogy is controversial for both its accuracy and its political motivation.
- **Distribution of pirated software:** It means distributing pirated software from one computer to another intending to destroy the data and official records of the government.
- **Possession of Unauthorized Information:** It is very easy to access any information by the terrorists with the aid of internet and to possess that information for political, religious, social, ideological objectives.

4. Cybercrimes against Society at large:

An unlawful act done with the intention of causing harm to the cyberspace will affect large number of persons. These offences includes:

- **Child Pornography:** It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children. It also includes activities concerning indecent exposure and obscenity.
- **Cyber Trafficking:** It may be trafficking in drugs, human beings, arms weapons etc. which affects large number of persons. Trafficking in the cyberspace is also a gravest crime.
- **Online Gambling:** Online fraud and cheating is one of the most lucrative businesses that are growing today in the cyber space. There are many cases that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs, etc.
- **Cyber Phishing :** It is a criminally fraudulent process in which cyber criminal acquires sensitive information such as user name, passwords and credit card details by disguising as a trustworthy electronic communication.
- **Web Jacking :** The term refers to forceful taking of control of a web site by cracking the pass word.
- **Spamming :** It is sending of unsolicited bulk and commercial messages over the internet all though irritating it is not illegal unless it causes damages of overloading network and disrupt the service.
- **Financial Crimes:** This type of offence is common as there is rapid growth in the users of networking sites and phone networking where culprit will try to attack by sending bogus mails or messages through internet. Ex: Using credit cards by obtaining password illegally.

VOLUME 2 | ISSUE 1 | ISSN 2456-9704

- **Forgery:** It means to deceive large number of persons by sending threatening mails as online business transactions are becoming the habitual need of today's life style.

Introduction :
The Term Cyber Security is used to refer security offered through on – line services to project your on – line information.

Cyber Security : Cyber Security means internet security is a branch of computer security specifically related to internet, is object is to establish rules and measures to use against attacks over the internet.

Need of Cyber Security :
Cyber security is necessary since it helps in securing data from threats such as theft or misuse, also safeguard your system from viruses.

- The Cyber Security will defend us from critical attack.
- It helps us to browse the safe website.
- It process all the incoming and outgoing data on our computer.
- Cyber Security will defend from hacks and virus.
- The Cyber Security developed will update their database very weak once. Hence the new virus also deleted.

Viruses and worms :
A virus is a program that is loaded onto your computer without your knowledge and runs against your wishes.

Solution :
Install a security suit that protects the computer against threats such as viruses and worms.

Hackers :
In common a hacker is a person who breaks into computers, usually by gaining access to administrative controls.

Types of Hackers :
White hat hacker : A WHH is a computer security expert and ethical hacker who breaks the protected systems and network.

Black Hat Hacker : Crackers or dark side hacker is an individual with extensive computer knowledge whose purpose is to breach or bypass internet security. They may steal or modify data or insert viruses or worms which damage the system.

Grey hat hacker : Are often hobbyists with intermediate technical skills, dabble in minor white collar crimes. They will hack into networks, stand alone computers and software.

How to present hacking :
It is very difficult to prevent computer hacking using passwords and firewalls can help to prevent.

Malware : It is derived from the term "malicious soft ware". Malware is software that infects and damages a computer system without the owner's knowledge or permission.

To stop Malware :

- Download an anti-malware program that also helps prevent infections.
- Activate network threat protection

VOLUME 2 | ISSUE 1 | ISSN 2456-9704

firewall, antivirus.

Trojan horses:

- Trojan horses are email viruses that can duplicate themselves, steal information, or harm the computer system.
- These viruses are the most serious treats to computers

How to avoid Trojans:

- Security suites, such as Avast means protect your devices with the best free antivirus on the market.
  Internet security will prevent you from downloading Trojan horses.

Password Cracking : Passwords attacks to different protected electronic areas and social network sites.

Security password :

- Use always strong password.
- Never use same password for 2 different sites.

Cyber security is everyone's responsibilities :

India stands 10th in the cyber crime in the world.
USA is 1st

Privacy Policy :
Before submitting your name email, address on a website look for the sites privacy policy.

Keep software up to date : Use difficult password.

Anti – Stalking tips :

- Maintain vigilance over physical access to your computer and other web – enabled devices like cell phone.
- Use always logout of your computer programs when you step away from the computer.
- Use the privacy settings in all your online accounts to limit your online sharing.
- Make sure to practice good password management and security.

Preventive Measures For Cyber Crimes:

Prevention is always better than cure. A netizen should take certain precautions while operating the internet and should follow certain preventive measures for cyber crimes which can be defined as:

- Identification of exposures through education will assist responsible companies and firms to meet these challenges.
- One should avoid disclosing any personal information to strangers via e-mail or while chatting.
- One must avoid sending any photograph to strangers by online as misusing of photograph incidents increasing day by day.
- An update Anti-virus software to guard against virus attacks should be used by all the netizens and should also keep back up volumes so that one may not suffer data loss in case of virus contamination.
- A person should never send his credit card number to any site that is

VOLUME 2 | ISSUE 1 | ISSN 2456-9704

not secured, to guard against frauds.

- It is always the parents who have to keep a watch on the sites that your children are accessing, to prevent any kind of harassment or depravation in children.
- Web site owners should watch traffic and check any irregularity on the site. It is the responsibility of the web site owners to adopt some policy for preventing cyber crimes as number of internet users are growing day by day.
- Web servers running public sites must be physically separately protected from internal corporate network.
- It is better to use a security programmes by the body corporate to control information on sites.
- Strict statutory laws need to be passed by the Legislatures keeping in mind the interest of netizens.
- IT department should pass certain guidelines and notifications for the protection of computer system and should also bring out with some more strict laws to breakdown the criminal activities relating to cyberspace.
- As Cyber Crime is the major threat to all the countries worldwide, certain steps should be taken at the international level for preventing the cybercrime.
- A complete justice must be provided to the victims of cyber crimes by way of compensatory remedy and offenders to be punished with highest type of punishment so that it will anticipate the criminals of cyber crime.

Safety tips to Cyber Security :

- Realize that you are an attractive target to hackers. Don't ever say "It won't happen to me."
- Practice good password management. Use a strong mix of characters, and don't use the same password for multiple sites. Don't share your password with others, don't write it down, and definitely don't write it on a post-it note attached to your monitor.
- Never leave your devices unattended. If you need to leave your computer, phone, or tablet for any length of time—no matter how short—lock it up so no one can use it while you're gone. If you keep sensitive information on a flash drive or external hard drive, make sure to lock it up as well.
- Always be careful when clicking on attachments or links in email. If it's unexpected or suspicious for any reason, don't click on it. Double check the URL of the website the link takes you to: bad actors will often take advantage of spelling mistakes to direct you to a harmful domain. Think you can spot a phony website? Try our Phishing Quiz.
- Sensitive browsing, such as banking or shopping, should only be done on a device that belongs to you, on a

network that you trust. Whether it's a friend's phone, a public computer, or a cafe's free WiFi—your data could be copied or stolen.

- Back up your data regularly, and make sure your anti-virus software is always up to date.
- Be conscientious of what you plug in to your computer. Malware can be spread through infected flash drives, external hard drives, and even smartphones.
- Watch what you're sharing on social networks. Criminals can befriend you and easily gain access to a shocking amount of information—where you go to school, where you work, when you're on vacation—that could help them gain access to more valuable data.
- Offline, be wary of social engineering, where someone attempts to gain information from you through manipulation. If someone calls or emails you asking for sensitive information, it's okay to say no. You can always call the company directly to verify credentials before giving out any information.
- Be sure to monitor your accounts for any suspicious activity. If you see something unfamiliar, it could be a sign that you've been compromised.

Case Studies on Cyber Crime :

Case law :Satyam Infoway ltd Vs Silfynet solutions Pvt

2004(3) AWC 2366 SC

In this case, SC pronounced that the Indian Trade Marks Act, 1999 is applicable to the regulation of domain names.The decision in favour of Satyam Infoway was premised on the court's observation that domain names may have all the features of traemarks. The court observed the confusion in identical of domain names. In that situation instead of being directed to the website of the legitimate owner of the name, a user could be divete to the website.

State of Tamil Nadu vs Subus Katti

In this case, a woman complained to the police about a man who was sending her obscene, defamatory and annoying messages in a Yahoo message group. the accused also forwarded emails received in a fake account opened by him in the victim's name. The victim also received phone calls by people who believed she was soliciting for sex work

The accused is found guilty of offences under section 469. 509 IPC and 67 of IT Act 2000 and the accused is convicted and is sentenced for the offence to undergo rigorous imprisonment for 2 years under 469 IPC and to pay fine of Rs 500/- and for the offence U/S 509 IPc sentenced to undergo 1 year simple imprisonment and to pay fine of Rs 500 and for offence u/s67 of IT Act 2000 to undergo rigorous imprisonment for 2 yrs and to pay fine Rs. 4000/-

Important Sections inserted by the IT Amendment Act 2008

Section 43A - Compensation for

VOLUME 2 | ISSUE 1 | ISSN 2456-9704

failure to protect data.

Section 66 - Computer related Offences

Section 66A - Punishment for sending offensive messages through communication service,etc.

section 66B - Punishment for dishonestly receiving stolen computer resource or communication device.

Section 66C - Punishment for identify theft

Section 66D - Punishment for cheating by personation by using computer resource

section 66E - Punishemnt for violation for privacy

Section 66F - Punishment for cyber terrorism

Section 67 - punishment for publishing or transmitting of material in electronic form

Section 67A -Punishment for publishing or transmitting of material containing sexually explicit act, etc, in electronic form.

- Section 67B - Punishment for publishing or transmitting of material depiciting children in sexually explicit act, etc in electronic form
- Section 67C - Preservation and retention of information by intermediaries
- Section 69 - Powers to issue directions for interception or monitoring or decryption of any information through any computer resource.
- Section 69A - Power to issue directions for blocking for public access of any information through and computer resource.
- Section 69B - Power to authorize to monitor and collect traffic data or information through any computer resource for cyber security
- section 72A - Punishment for disclosure of information in breach of lawful contract
- section 79 -exemption from liability of intermediary in certain cases
- Section 84A - Modes or methods for encryption
- section 84B - Punishment for abetment of offences
- Section 84C - Punishment for attempt to commit offences.

Kenneth L. Haywood :

Kenneth L. Haywood (born 1964) became involved in a 2008 controversy in the Indian city of Mumbai after his wireless connection was allegedly used by terrorists to transmit a message to Indian news networks before their attacks. It was subsequently revealed that Haywood had been living a double life as an "executive skills trainer" and a Christian pastor, while the firm that he worked for was a probable front for evangelical religious activities. Haywood was not charged by Indian authorities in connection with the blasts, which occurred at Ahmedabad and Surat, in late July 2008.

Cyber pornography :

Some more Indian incidents revolving around cyber pornography include the Air Force Balbharati School case. In the first case of this kind, the Delhi Police Cyber Crime Cell registered a case under section 67 of the IT act, 2000. A student of

VOLUME 2 | ISSUE 1 | ISSN 2456-9704

the Air Force Balbharati School, New Delhi, was teased by all his classmates for having a pockmarked face.

Cyber stalking :

Ritu Kohli has the dubious distinction of being the first lady to register the cyber stalking case. A friend of her husband gave her telephonic number in the general chat room. The general chatting facility is provided by some websites like MIRC and ICQ. Where person can easily chat without disclosing his true identity. The friend of husband also encouraged this chatters to speak in slang language to Ms. Kohli.

Important case studies in India :

A complaint was filed in by Sony India Private Ltd, which runs a website called sony-sambandh.com, targeting Non Resident Indians. The website enables NRIs to send Sony products to their friends and relatives in India after they pay for it online.

The company undertakes to deliver the products to the concerned recipients. In May 2002,someone logged onto the website under the identity of Barbara Campa and ordered a Sony Colour Television set and a cordless head phone.A lady gave her credit card number for payment and requested that the products be delivered to Arif Azim in Noida. The payment was duly cleared by the credit card agency and the transaction processed. After following the relevant procedures of due diligence and checking, the company delivered the items to Arif Azim.

At the time of delivery, the company took digital photographs showing the delivery being accepted by Arif Azim.

The transaction closed at that, but after one and a half months the credit card agency informed the company that this was an unauthorized transaction as the real owner had denied having made the purchase.

The company lodged a complaint for online cheating at the Central Bureau of Investigation which registered a case under Section 418, 419 and 420 of the Indian Penal Code.

The matter was investigated into and Arif Azim was arrested. Investigations revealed that Arif Azim, while working at a call centre in Noida gained access to the credit card number of an American national which he misused on the company's site.

The CBI recovered the colour television and the cordless head phone.

The accused admitted his guilt and the court of Shri Gulshan Kumar Metropolitan Magistrate, New Delhi, convicted Arif Azim under Section 418, 419 and 420 of the Indian Penal Code — this being the first time that a cyber crime has been convicted.

The court, however, felt that as the accused was a young boy of 24 years and a first-time convict, a lenient view needed to be taken. The court therefore released the accused on probation for one year.

Case-2: First juvenile accused in a cyber crime case.

VOLUME 2 | ISSUE 1 | ISSN 2456-9704

In April 2001 a person from New Delhi complained to the crime branch regarding the
website. Amazing.com, he claimed, carried vulgar remarks about his daughter and a few of her classmates. During the inquiry, print-outs of the site were taken and proceedings initiated.

After investigation a student of Class 11 and classmate of the girl was arrested.

The juvenile board in Nov 2003 refused to discharge the boy accused of creating a website with vulgar remarks about his classmate.

The accused's advocate had sought that his client be discharged on the ground that he was not in a stable state of mind. Seeking discharge, the advocate further said that the trial has been pending for about two years.

While rejecting the accused's application, metropolitan magistrate Santosh Snehi Mann said: 'The mental condition under which the juvenile came into conflict with the law shall be taken into consideration during the final order.' Mann, however, dropped the sections of Indecent Representation of Women (Prohibition) Act.

The accused would face trial under the Information Technology Act and for intending to outrage the modesty of a woman. She held the inquiry could not be closed on technical ground, especially when the allegations were not denied by the accused.

Case 3: First case convicted under Information Technology Act 2000 of India.

The case related to posting of obscene, defamatory and annoying message about a divorcee woman in the yahoo message group. E-Mails were also forwarded to the victim for information by the accused through a false e-mail account opened by him in the name of the victim. The posting of the message resulted in annoying phone calls to the lady in the belief that she was soliciting.

Based on a complaint made by the victim in February 2004, the Police traced the accused to Mumbai and arrested him within the next few days. The accused was a known family friend of the victim and was reportedly interested in marrying her. She however married another person. This marriage later ended in divorce and the accused started contacting her once again. On her reluctance to marry him, the accused took up the harassment through the Internet.

On 24-3-2004 Charge Sheet was filed u/s 67 of IT Act 2000, 469 and 509 IPC before The Hon'ble Addl. CMM Egmore by citing 18 witnesses and 34 documents and material objects. The same was taken on file in C.C.NO.4680/2004. On the prosecution side 12 witnesses were examined and entire documents were marked. The Defence argued that the offending mails would have been given either by ex-husband of the complainant or the complainant her self to

VOLUME 2 | ISSUE 1 | ISSN 2456-9704

implicate the accused as accused alleged to have turned down the request of the complainant to marry her. Further the Defence counsel argued that some of the documentary evidence was not sustainable under Section 65 B of the Indian Evidence Act. However, the court based on the expert witness of Naavi and other evidence produced including the witness of the Cyber Cafe owners came to the conclusion that the crime was conclusively proved.

The court has also held that because of the meticulous investigation carried on by the IO, the origination of the obscene message was traced out and the real culprit has been brought before the court of law. In this case Sri S. Kothandaraman, Special Public Prosecutor appointed by the Government conducted the case.

Honourable Sri.Arulraj, Additional Chief Metropolitan Magistrate, Egmore, delivered the judgement on 5-11-04 as follows:

"The accused is found guilty of offences under section 469, 509 IPC and 67 of IT Act 2000 and the accused is convicted and is sentenced for the offence to undergo RI for 2 years under 469 IPC and to pay fine of Rs.500/-and for the offence u/s 509 IPC sentenced to undergo 1 year Simple imprisonment and to pay fine of Rs.500/- and for the offence u/s 67 of IT Act 2000 to undergo RI for 2 years and to pay fine of Rs.4000/- All sentences to run concurrently."

Conclusion :

Since users of computer system and internet are increasing worldwide, where it is easy to access any information easily within a few seconds by using internet which is the medium for huge information and a large base of communications around the world. Certain precautionary measures should be taken by netizens while using the internet which will assist in challenging this major threat Cyber Crime.

Cyber Security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attacks, damage or unauthorized access. In a computing context, security includes both Cyber Security and Physical Security.

"Technology is destructive only in the hands of people who do not realize that they are one and the same process as the universe".

"Think before you click, care to be aware".

Reference :

1. **Cyber law Indian and International Perspectives.**

By : Aparna Viswanathan, Published by : Lexis Nexis

2. Cracking Code Book : By Simon Sing

- http://it.slashdot.org/article.pl?sid=07/09/19/036203
- http://www.dnaindia.com/money/report_antivirus-war-hots-up-with-monthly-plans_1198789
- http://www.isc2.org/PressReleaseDetails.aspx?id=3238

- The 2009 "Tour of Cyber Crimes" by Joe St Sauver, Ph.D. (joe@uoregon.edu), http://www.uoregon.edu/~joe/cybercrime2009/
- http://www.newworldencyclopedia.org/entry/Cybercrime#Credits
- http://www.newworldencyclopedia.org/entry/Cybercrime#Credits
- http://www.cbintel.com/AuctionFraudReport.pdf
- http://searchcrm.techtarget.com/sDefinition/0,,sid11_gci1000478,00.html
- http://www.state.gov/www/regions/africa/naffpub.pdf
- http://ezinearticles.com/?Reshipping-Fraud---A-Home-Business-Con&id=582426
- http://www.paid-survey-success.com/online-scams-high-yield-investment-programs-hyip/
- http://www.consumerfraudreporting.org/Education_Degree_Scams.php
- http://www.healthwatcher.net/dietfraud.com/Dietcraze/scams_belldietpatch.html
- http://reviews.ebay.com/BEWARE-COUNTERFEIT-ITEMS-BEING-SOLD-AS-AUTHENTIC_W0QQugidZ10000000004551474
- http://www.smokersclubinc.com/modules.php?name=News&file=article&sid=2373
- http://www.theregister.co.uk/2002/03/28/online_gambling_tops_internet_card/
- http://www.usatoday.com/sports/2007-04-27-internet-gambling-bill_N.htm
- http://www.forbes.com/forbes/2006/0327/112.html and http://www.forbes.com/lists/2006/10/GCUD.html
- Links to the following case studies on Cyber Crime were provided by Mr. Jay Srinivasan Head, Governance & Assurance, Fidelity India
- Following case studies on Cyber Crime were provided by Dr. Uma Somayajula, an eminent IT Security professional and DSCI member

Following case studies on Cyber Crime were provided by Dr. Uma Somayajula, an eminent IT Security professional and DSCI member.

*****