ISSN : 2231-0711

K.Krishna Jyothi et al | International Journal of Computer Science Engineering and Technology(IJCSET) | Dec 2014 | Vol 4, Issue 12,376-383

Approaches and Scenarios to Combat Cyber Crime

K.Krishna Jyothi[1#], G. Kalyani[2#],Prof.T.Venkat Narayana Rao[3#]

Assistant Professor[1#], Assistant Professor[1#], Professor[3#]
Department of Computer Science and Engineering
Sreenidhi Institute of Science and Technology
R.R District, T.S, India

Abstract –In the recent day's usefulness and importance of the internet has become a new crime tool. This paper focuses on different types of cyber crimes namely: phishing, email spoofing and cyber pornography. It provides a review of cyber crimes and the means to protect from such crimes. The study looks at areas related to cybercrime at present and to review criminological theories that have been applied to the study of cybercrime. Our world only two decades old in terms of digital age, and our understanding of cybercrime is continually changing by looking at our understanding of cybercrime and cyber oppression . The laws are stringent and the enforcement is steady but due to advent of technology all the efforts to crimes are in vain. Crime is no longer restricted to space, time or a set of natives. The cases and exemplars offers a detail narration of real-time cases transpired in Indian and overseas context. The readers would avail a detailed account of kinds of crimes, laws/ acts and section to deal with such crimes.

Keywords : offence, service, secret, cyber, attacks.

I. INTRODUCTION

A crime committed or facilitated via the Internet is a cybercrime. Cybercrime is also called as online computer crime. Cybercrime is any criminal activity involving computers and networks. It can range from fraud to unwanted emails (spam) to online banking system breach. It can include the distant theft of government or corporate resources through a offender intruding into remote systems around the globe. Cybercrime may also include non-monetary offenses, such as creating viruses on other computers or posting private business information on the Internet [2]. Cyber crime is all derived from the term "cyber space" itself. Cyberspace is "the speculative environment in which message over computer networks occurs. In the recent days the network traffic has risen drastically and hence digital data has grown vividly and the term "cyberspace" was able to represent the many new ideas and phenomena that were emerging. Therefore, cyber security is the service offered to the cyberspace. Most of the cybercrimes are the attacks on information relating to individuals, corporations and governments. Although the attacks do not take place on a individual or commercial body, but it results in misuse of informational attributes belonging to people and institutions using Internet.

A. Losses due to cyber crime

- The loss of intellectual property and business confidential information
- Fraud ruining hundreds of millions of dollars every year
- Loss of susceptible business information, including possible stock market exploitation
- Loss of cost of efforts in services, employment disruptions, and reduced confidence for online activities
- Additional cost for securing networks, insurance, and recovery from cyber attacks
- Loss of reputation due to hacked corporation.

B. Relation Among Cyber Crime And Attacks

There are a number of techniques to combat cyber-attacks and there are plenty of ways to control. Attacks are broken down into two ways, Syntactic attacks and Semantic attacks. Syntactic attacks are clear-cut; it is considered wicked software which includes viruses, worms, and Trojan horses.

Semantic attack is the modification and diffusion of correct and incorrect information. To set someone into the wrong direction or to cover your tracks, the diffusion of incorrect information can be utilized.

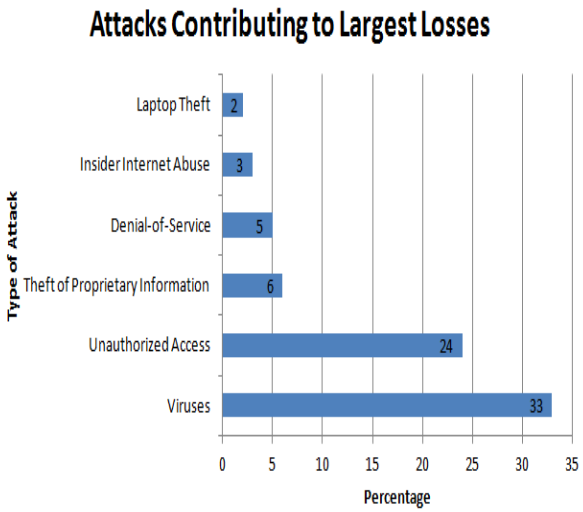

Figure 1: Types and extent of vulnerability of crimes

Based on the data taken from the CSI/FBI 2005, as shown in the figure 1, the computer crime surveys depicts that the losses due unauthorized access and viruses is more that has caused loss in businesses and theft of intellectual properties.

II. TYPES OF CYBER CRIME

The frequent kinds of cyber crimes could be:

A. *Hacking* - A hacker is an unofficial user who attempts to or gain entry into an information system. Hacking is a subtle crime which is not noticeable by the system, and causes an assault to the privacy of data. There are different categories of Hackers.

i) White Hat Hackers - They believe that information giving out is good and right. Such users are very termed as "joy rider " on PC and are very harmful.

iii) Black Hat Hackers - They cause damage by initiating interruption. They may steal or alter data or insert viruses or worms which is harmful to the system. They are also called 'crackers'.

iv) Grey Hat Hackers - Typically moral but seldom violates hacker moral values. Hackers will sliver the networks, stand-alone computers and software. Network hackers attempt to gain illegal access to private computer networks just for dispute, snooping, and allocation of information. Crackers perform illegal interruption with damage like pinching or altering of information or inserting malware (viruses or worms)

B. Cyber Stalking - This crime involves use of internet to hassle someone. The activities includes fake accusations, intimidation etc. Normally, common of cyber stalkers are men and the majority of fatalities are women [1].

C. Spamming - Spamming is a process of transmitting unwanted mass and money-making messages over the internet. Although frustrating to most email users, it is not illegal except it causes harm such as overfilling network and distracting service to subscribers or creates negative impact on the user attitudes towards Internet Service Provider.

D. Cyber Pornography - Women and children are victims of sexual abuse through internet. Pedophiles use the internet to mail photos of illegitimate child pornography to embattled children so as to draw children to such funs. Afterwards they are sexually demoralized for gains.

E. Phishing - It is a unlawfully falsified process of acquiring susceptible information such as username, passwords and credit card details by disguising as a truthful entity in an electronic communication[2][1].

F. Software Piracy - It is an illegal reproduction and division of software for business or individual use. This comes under violation of copy right and a violation of a license accord. Since the unauthorized user is not a party to the license pact and it is complicated to locate out remedies for such offence.

G. Corporate Espionage - **I**t is an offence of secrets such as cable taps or illegitimate intrusions in or outside organization.

H. Money Laundering - It is an evil of illicitly acquired cash through lawful means. Such as transport cash to a country bypassing rigid banking policy and move it back by means of loans. The interest of which can reduced from his taxes. This is possible earlier to computer and internet technology; electronic transfers have made it easier and more triumphant.

I. Embezzlement - Unlawful stealing of money, property or any other thing of worth that has been entrusted to the offender's concern, guardianship or control is called embezzlement. Internet facilities are distorted to obligate this crime.

J. Password Sniffers - Password sniffers are programmers that scrutinize and witness the name and password of network users as they log in, jeopardizing protection at a site. Whoever installs the sniffer can masquerade as an authorized user and log in to access on confidential credentials.

K. Spoofing - It is the work of disguising one computer to electronically "appear" like another computer, in order to gain admittance to a system that would be usually is controlled. Spoofing was used to access exclusive data stored in a computer belonging to security expert.

L. Credit Card Fraud - It is the illicit use of a credit/debit card to deceptively gain money or assets. Credit/debit card numbers can be stolen from unsecured web sites, or can be obtained in a distinctiveness theft plan.

M. Web Jacking - The term refers to influential captivating of control of a web site by fabricating the password.

N. Cyber terrorism - The use of computer assets to frighten or oblige government, the citizens or any sector is called cyber terrorism. Individuals and groups quite often try to exploit nameless character of the internet to pressure governments and terrorize the citizens of the country[4].

III. CYBER ACTS AND LAWS

In India the Information Technology Act 2000 was approved to offer legal identification for dealings carried out by means of electronic communication. The Act deals with the law relating to Digital Contracts, Digital assets, and Digital privileges and any defiance of these laws constitutes an offense. The Act stipulates very high punishments for such crimes. The Information Technology (amendment) Act, 2008(Act 10 of 2009), has further improved the punishments. Life imprisonment and fine up to rupees ten lakhs could be specified for definite classes of cyber crimes. Compensation up to rupees five crores can be given to affected persons if harm is made to the computer, computer system or computer network by the beginning of virus, denial of services etc.(**S. 46(1-A)**). Sections **65-74** the Act particularly deals with sure offences, which can be called Cyber Crimes [3]. A detail account of all offences and cyber laws is depicted in Table I and II in the context of Indian and American countries[5][6].

IV. CYBER CASES

A. Purchase Order Scam

This offense surfaced in U.S in the year 2014, where in African cyber criminals have devised a scheme that had cost U.S. retailers millions dollars. Through online and telephone social engineering techniques, the fraudsters trapped the retailers into believing they are from authentic businesses and educational institutions and wanted users to order the products. The retailers filled the requirements, but the goods end up being delivered elsewhere. It often seen that the unsuspicious at-home Internet users, who are duped into re-shipping the goods to other countries.

"They order bulk quantities of items such as laptops and hard drives," said Special representative Joanne Altenburg, who is investigating the cyber criminals since 2012 . The

fraudsters usually order expensive and very specialized tools, such as costly equipments , peripherals, medicinal and pharmaceutical items. The investigators have found more than 85 companies and universities nationwide whose identities were used to commit the plan. Approximately 400 actual attempted incidents have harassed some 250 vendors, and nearly $5 million has been lost so far.

The scam has some variations, but basically it works like this:

- The criminals set up fake websites with domain names nearly indistinguishable to those of real businesses or universities. They do the same for e-mail accounts and as well use telephone spoofing techniques to make calls emerge to be from the right area codes.
- Next, the fraudsters pretend as school or business officials and contact a retailer's customer service center and use social engineering strategy to gather information about the organization's purchasing report.
- The criminals then contact the target business houses and ask for a quote for goods. They use forged documents, complete with letterheads and sometimes even the name of the organization's actual product manager. They request that the shipments be made on a 30-day credit and since the real institution often has good credit, vendors typically agree.
- The criminals provide a U.S. shipping address that might be a warehouse, self-storage facility, or the residence of a victim of an online romance or work-from-home scam. Those at-home victims are directed to re-ship the merchandise to fraudster's native country and are provided with shipping labels to make the job easy.
- The vendor lastly bills the real organization and realizes the scam. By then, the items have been re-shipped overseas, and the retailer must accept the financial loss.

B. GameOver Zeus Botnet Disrupted

Gameover Zeus is a malware that has occurred on in June 2014 that has made multinational effort disruption i.e. a malicious software that has stolen millions around the world. GameOver Zeus is an extremely complicated type of malware intended exclusively to steal banking and other credentials from the computers it infects. It's had predominately reached through spam e-mail or phishing messages. In the case of GameOver Zeus, its primary rationale is to capture banking credentials from infected computers, then use those credentials to begin or forward wire transfers to accounts abroad that are controlled by the criminals. Victims attributed to GameOver Zeus are expected to be more than $100 million.

C. *Sex Trafficker Receives 40-Year Sentence*

In January/2014 in Texas a man trapped young victims through Social Media Sites are yet another vital example of how social media can be hazardous for young people. Newly, a resident of Houston was sentenced to 40 years in prison on child sex trafficking charges, the modus operandi adapted was to identifying and contacting young girls to cheat through social media platforms The case was investigated by the FBI's Child Exploitation Task Force in Houston, one of many child focused task services. This agency is still working next to other partner agencies to explore individuals and criminal enterprises liable for victimizing juvenile people. The Houston task force works closely with the Houston Police Department in particularly, its Vice and Juvenile Sex Crimes Divisions and officers who recovered one of Harris' victims and subsequently notified the task force.

The task force collected enough proofs to argue Harris to appeal guilty. There were also enough proofs to prompt the judge to order that after serving his 40-year sentence Harris spend the rest of his life under supervision[5].

D. On line credit card scam

This is most common cyber crime and the apathy is that it is still a ongoing crime. In this the Customer's credit card details are misused through online means for booking any commodity such air-tickets or any online product or service. For example such culprits were wedged by the city Cyber Crime Investigation Cell in Pune recently. It is found that details altered belonging to 100 people [4]. ICICI Prudential Life Insurance officer had complained in support of one of his customer. In this regard 3 people were arrested. These criminals were aware and were employed with financial intuitions and bank.

According to the information provided by the police, one of the customers received a SMS based alert for purchase of the ticket even when the credit card was being held by him. Customer was attentive and came to identify something was suspicious; he enquired and came to know about the fraud. He contacted the bank and narrated the incident. The police departments had observed that all banks are subjected to the same.

The tickets were book through online means. Police requested for the log information and got the information of the Private Institution. Investigation exposed that the details were obtained from the bank. The accused was working in the credit card department; and had access to credit card details of few clients. He had given few tickets to different other institutions. The police department have been taking such crimes very seriously and had initiated special training sessions to enable their supervising /vigilance personnel to make them aware of such incidents and how to monitor/ arrest such frauds and fraudsters.

V. METHODS TO PREVENT CYBERCRIME

Indicators of Fraud

Businesses can stay away from becoming sufferers of purchase order fraud by being conscious of number of deception indicators:

- Flawed domain names on websites, e-mails, and acquisition orders. The scammers use almost identical domain names of officially authorized organizations, but in the case of an institution of higher education, for example, if the URL does not end in .edu, it is likely deceiving site.
- The shipping address on an acquisition order is not the same as the business site. Similarly, if the delivery

address is a residence or self-storage facility, it must elevate red flags.

- Weakly written e-mail correspondence that contains grammatical mistakes, suggesting that the message was not written by a fluent English speaker.
- Phone numbers not related with the company or university, and numbers that are not answered by anyone
- Orders for unusually large quantities of products, with a appeal to ship priority or overnight.

If you are the sufferer of purchase order deception, it's must to contact local law enforcement and the FBI. You should also indicate the crime to the Internet Complaint Center (IC3). If the fraud is discovered before the merchandise are shipped to other location, there is a possibility that the goods can be recovered. More than $1 million valued of goods has been recovered so far after quick discovery of the fraud[4].

B. How to Identify our computer is being compromised

- Your computer system operates extremely slowly.
- Your cursor moves unsteadily with no input from you.
- You notice informal logins to your bank accounts or informal money transfers.
- Text-based chat windows emerge on your computer's desktop unexpectedly.
- Your computer records lock up and a payoff demand is made to unlock records.

If you watch one or more of these events on your computer, you may have been polluted with the GameOver Zeus malware. Security experts are advising that businesses go on to offer guidance to users to teach them not to click on aggressive or suspicious links in emails or Web sites.

C. Basic ways to prevent cyber crime

Basing on popular adage "information is power," and it is true when it comes to cybercrime. Access to your individual information is what gives hackers the authority to tap into your financial records and steal your money or your identity. But the right information can also permit you to guard yourself from being trapped in the cybercrime.
Following are the domain specific steps to be considered to avoid becoming a sufferer of cybercrime.

a. *Education* - Hackers aren't the only ones who can increase authority from information. By refining yourself about the types of frauds that exist on the Internet and how to prevent them, you are putting yourself one step forward of the cybercriminals. Since phishing is common, read up on the latest phishing frauds and learn how to identify a phishing attempt. Consider, phishing is when hackers try to attract you into revealing personal information by pretending to be a valid organization or person. These scams often have fun off major new stories, so keep informed on the latest news-related scams.

b. *Use a firewall* - Firewalls ensure transfer between your computer or network and the Internet and serve as a great first line of protection when it comes to keeping intruders away Hence , usage of firewall is mandatory for formal and informal tasks. And if you have a residence wireless network, use the firewall that comes with your router[3].

c. *Click with caution* - When you're inspection your email or chatting over instant messenger (IM), be watchful not to select any links in messages from the one you are not aware off. The link might take you to a fake website that would ask your confidential information, such as user names and passwords, or it might download malware on the computer. If the message is from somebody you know, be careful. A few viruses duplicate and would reach through email, so ensure that the information that indicates that the message is valid.

d. *Practice safe surfing* - While navigating the web, you need to take safety measures to avoid fake websites that solicit your private information and pages that include malware. Use a search engine to assist you to navigate to a proper web address. That way, you won't wind up on a phony page or a generally misspelled address. Creating a fake site at an address similar to the actual site is called "typo squatting," and it is quite a frequent scam.

e. *Practice safe shopping* - In addition to practicing safe surfing, it is vital to be vigilant while shopping online. One must be careful when shopping at a site that you've not visited previous to and do a little inquisition before you enter your imbursement information. Look for a Trustmark, such as McAfee SECURE and when you're on a payment page, look for the lock sign in your browser, representing that the site uses encryption, or scrambling, to keep your data safe. Click on the icon to make sure that the security certificate pertains to the site. Check for the address bar, if the site starts with "https://" instead of http:// because this is an additional way to see if the site uses encryption. When about to pay, use a credit card as an alternative of a debit card. If the site turns out to be deceptive your credit card issuer may reimburse you for the charges, which can't done for usage of debit card . Finally, assess the site's security and privacy policies mentioned on the site.

f. *Use complete security software and keep your system updated* - Hackers have a wide variety of methods into system and information; the need to have complete security software that can protect the user from all directions. It is advisable to keep the security software is up to date by selecting the automatic update option on your security control panel. Regular scans are must to safe guard the operating system (OS), browser and data with the newest security patches.

g. *Secure your wireless network* - Hackers can access data while it's in transfer on an unsecured wireless network. The hackers can be set aside out by enabling the firewall on the router and alter the router's administrator password periodically. Cybercriminals

often know the evade passwords and they use them to hack into the network. The administrators must ensure to set up a router so that it only allow access to people with passwords that are encrypted. Check owner's manual for commands on setting up encryption.

h. *Use tough passwords* - Even though it may be easier to remember short passwords that reference birthday, middle name, or pet's name but these kinds of passwords also make it effortless for hackers to do offences. Strong passwords can go an extended way in helping secure the information, so choose a password that is at least 10 characters lengthy and consists of an arrangement of letters, numbers and special characters. Also consider altering the password sporadically to reduce the probability of it being compromised.

i. *Use common sense* - In spite of caution, cybercrime is increasing, fueled by regular mistakes people respond to spam and downloading attachments from people they don't know. So, use common wisdom when using Internet. Never post personal data online or share sensitive information such as your social security number and credit card number or personal details. Exercise vigilance when clicking on any links or downloading any programs.

j. *Be suspicious* - Even if considered to be cyber know-how, still one must need to keep the guard up for any new tricks and be practical about safety issues. Backup the data habitually in case anything goes wrong, and monitoring the accounts and credit reports to make sure that a hacker has not stolen the data or identity. Although defending does take some endeavor, remember that there are a set of resources and tackles to be safe. And by adopting a few safety measures and best practices, it can help in keeping away from cybercrime.

k. Stay safe online on social media

- Connect to only "friend" or people that are know online personally.
- Set public media security settings so that only confirmed friends and connections can see what are being posted.
- Never place a photograph of yourself or write anything on social media sites or in e-mails and text messages seen by the world as public.
- Be wary of giving someone meet through social media , phone number, e-mail address, or residence address.
- Most importantly, be aware of anyone who meet online, but may not be the same whom you met online.

VI. TO WHOM WE NEED TO APPROACH

Internet related crime, like any other crime, should be reported to right law enforcement investigative authorities at the local, state, federal and international levels, depending on the extent of the crime. Citizens who are awake of centralized crimes should report them to local offices of federal law enforcement.

The federal law enforcement agencies that examine domestic crime on the Internet include:

- The Federal Bureau of Investigation (FBI)
- The United States Secret Service
- The United States Immigration and Customs Enforcement (ICE)
- The United States Postal Inspection Service
- The Bureau of Alcohol, Tobacco and Firearms (ATF).
- Cyber Crime Police Station, Crime Investigation Department, Hyderabad, India
- CBI Cyber Crime Cell, New Delhi, India

In general, a national crime may be reported to the local office i.e. an appropriate law enforcement agency.

VII. CONCLUSION

The risks of cyber crime are very real and too threatening to be ignored. In this paper it has focused on few cyber crimes that are existing and some are emerging in India and overseas. It is evident from the study that cyber crimes knowledge can be classified in 3 distinct areas: Cyber Laws (referred as Cyber laws), Education and Policy making. All the ways to deal cyber crimes either are having very less noteworthy effort or none in many countries. The lack of work need to be improved in order to set novel paradigms for combating the cyber attacks. It also discussed about how to prevent cyber crime in simpler way. This paper offers a outline of the growing cybercrime problem and reviews criminological theories that have been applied to the learn cybercrime types and victimization. It further provide a account of laws governing and defining the cybercrimes, their jurisdiction and the legal base to impeach such crimes in the interest of citizens at large.

REFERENCES

[1] Shrivastav "ICT Penetration and Cybercrime in India: A Review" International Journal of Advanced Research in Computer Science and Software Engineering 3(7), July - 2013, pp. 414-419

[2] Mathew, A.R. " Cyber crimes: Threats and protection" Networking and Information Technology (ICNIT), 2010 International Conference 11-12 June 2010

[3] Sahu, B. "Identify Uncertainty of Cyber Crime and Cyber Laws" Communication Systems and Network Technologies (CSNT), 2013 International Conference 6-8 April 2013

[4] Banday, M. Tariq ; "A study of Indian approach towards cyber security" Emerging Technology Trends in Electronics, Communication and Networking (ET2ECN), 2012 1st International Conference 19-21 Dec. 2012

[5] http://www.fbi.gov/news/stories/story-index/cyber-crimes

[6] http://www.cyberpolicebangalore.nic.in/gazette-notify.html

Assistant Professor K.Krishna Jyothi, received B.Tech in Computer science and Engineering from JNTU, Hyderabad, India, holds a M.Tech in Computer Science from JNTU, Hyderabad, A.P., India. She has 5 years of experience in Computer Science and Engineering areas pertaining to academics. She is presently working as Assistant Professor, Department of Computer Science and Engineering, Sreenidhi Institute of Science and Technology , Ghatkesar , R.R.Dist.,T.S, INDIA. She is currently working in the areas of advanced Programming languages, Database paradigms and Network Security. She can be reached at kogantikrishnajyothi@gmail.com.

Assistant Professor G.Kalyani, received B.Tech in Computer science and Engineering from JNTU, Hyderabad, India, holds a M.Tech in Computer Science from IETE, Hyderabad, A.P., India. She has 9 years of experience in Computer Science and Engineering areas pertaining to academics. She is presently working as Assistant Professor, Department of Computer Science and Engineering, Sreenidhi Institute of Science and Technology , Ghatkesar , R.R.Dist.,T.S, INDIA. . She is currently working in the areas of advanced Programming languages , Compiler Design , Network Security and Discrete structures. She can be reached at kalyani_ghanta@yahoo.co.in

Professor T.Venkat Narayana Rao, received B.E in Computer Technology and Engineering from Nagpur University, Nagpur, India, M.B.A (Systems), holds a M.Tech in Computer Science from Jawaharlal Nehru Technological University, Hyderabad, A.P., India and a Research Scholar in JNTUK. He has 23 years of vast experience in Computer Science and Engineering areas pertaining to academics and industry related I.T issues. He is presently working as Professor, Department of Computer Science and Engineering, Sreenidhi Institute of Science and Technology , Ghatkesar , R.R.Dist.,T.S, INDIA. He is nominated as an Editor and Reviewer to 45 International journals relating to Computer Science and Information Technology and has published 72 papers in international journals. He is currently working on research areas, which include Digital Image Processing, Digital Watermarking, Data Mining, Network Security and other emerging areas of Information Technology. He can be reached at tvnrbobby@yahoo.com

Table I. Cyber laws in India

Sl.No	Offences	Section Under IT Act
1.	Tampering with computer source Documents.	Sec.65
2.	Hacking with computer systems and Data Alteration.	Sec.66
3.	Sending unpleasant messages through communication service, etc.	Sec.66A
4.	Deceitfully receiving stolen computer resource or communication device	Sec.66B
5.	Identity theft.	Sec.66C
6.	Cheating by personation by using computer resource..	Sec.66D
7.	Violation of privacy.	Sec.66E
8.	Cyber terrorism.	Sec.66F
9.	Publishing or transmitting obscene material in electronic form	Sec .67
10.	Publishing or transmitting of material containing sexually explicit act, etc. in electronic form.	Sec.67A
11.	Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form.	Sec.67B
11.	Preservation and Retention of information by intermediaries.	Sec.67C
12.	Powers to issue directions for interception or monitoring or decryption of any information through any computer resource.	Sec.69
13.	Power to issue directions for blocking for public access of any information through any computer resource.	Sec.69A
14.	Power to empower to monitor and collect traffic data or information through any computer resource for Cyber Security.	Sec.69B
15.	Un-authorized access to protected system.	Sec.70
16.	Penalty for misrepresentation.	Sec.71
17.	Breach of confidentiality and privacy.	Sec.72
18.	Publishing fake digital signature certificates.	Sec.73
19.	Publication for deceitful purpose.	Sec.74
29.	Act to apply for offence or contraventions committed outside India.	Sec.75
21.	Compensation, penalties or confiscation not to interfere with other Punishment.	Sec.77
22.	Compounding of Offences.	Sec.77A
23.	Offences with three years imprisonment to be cognizable.	Sec.77B
24.	Exclusion from liability of intermediary in certain cases.	Sec.79
25.	Punishment for abetment of offences.	Sec.84B
26.	Punishment for attempt to commit offences.	Sec.84C
27.	Offences by Companies.	Sec.85

Note : Sec.78 of I.T. Act empowers Police Inspector to investigate cases falling under this Act		
28.	Sending threatening messages by e-mail.	Sec .503 IPC
29.	Word, gesture or act intended to abuse the modesty of a woman.	Sec.509 IPC
30.	Sending defamatory messages by e-mail.	Sec .499 IPC
31.	Bogus websites , Cyber Frauds.	Sec .420 IPC
32.	E-mail Spoofing.	Sec .463 IPC
33.	Making a false document.	Sec.464 IPC
34.	Forgery for intention of cheating.	Sec.468 IPC
35.	Forgery for purpose of harming reputation.	Sec.469 IPC
36.	Web-Jacking.	Sec .383 IPC
37.	E-mail Abuse.	Sec .500 IPC
38.	Punishment for criminal intimidation.	Sec.506 IPC
39.	Criminal intimidation by an anonymous communication.	Sec.507 IPC
40.	When copyright infringed:- Copyright in a work shall be deemed to be. Infringed	Sec.51
41.	Offence of infringement of copyright or other rights conferred by this Act. Any. person who intentionally infringes or abets the infringement of	Sec.63
42.	Enhanced penalty on second and ensuing convictions.	Sec.63A
43.	Knowing use of infringing copy of computer programme to be an offence	Sec.63B
44.	Obscenity	Sec. 292 IPC
45.	Printing etc. of grossly filthy or scurrilous matter or matter intended for Blackmail	Sec.292A IPC
46.	Sale, etc., of obscene objects to young person	Sec .293 IPC
47.	Obscene acts and songs	Sec.294 IPC
48.	Theft of Computer Hardware	Sec. 378
49.	Punishment for theft	Sec.379
50.	Online Sale of Drugs	NDPS Act
51.	Online Sale of Arms	Arms Act

Table II. Cyber laws in United States

Sl.No	Offences	Section
1	Fraud and related activity in connection with recognition documents, authentication features, and information	18 U.S.C. § 1028
2	Aggravated identity theft	18 U.S.C. § 1028A
3	Fraud and related activity with regard to the access devices	18 U.S.C. § 1029
4	Fraud and related activity with regard to the computers	18 U.S.C. § 1030
5	Fraud and related activity with regard to the electronic mail	18 U.S.C. § 1037
6	Fraud by wire, radio, or television	18 U.S.C. § 1343
7	Communications lines, stations, or systems	18 U.S.C. § 1362
8	Importation or transportation of obscene matters	18 U.S.C. § 1462
9	Transportation of obscene matters for trade or distribution	18 U.S.C. § 1465
10	Obscene visual representation of the sexual abuse of children	18 U.S.C. § 1466A
11	Sexual exploitation of children	18 U.S.C. § 2251
12	Certain activities relating to material relating to the sexual exploitation of minors	18 U.S.C. § 2252
13	Certain activities relating to material constituting or containing child pornography	18 U.S.C. § 2252A
14	Misleading domain names on the Internet [to deceive minors]	18 U.S.C. § 2252B
15	Misleading words or digital images on the Internet	18 U.S.C. § 2252C
16	Use of interstate facilities to transmit information about a minor	18 U.S.C. § 2425
17	Criminal infringement of a copyright	18 U.S.C. § 2319
18	Criminal offenses [relating to copyright]	17 U.S.C. § 506
19	Unauthorized publication or use of communications	47 U.S.C. 605

20	Use of interstate facilities to transmit information about a minor	18 U.S.C. § 2425
21	Criminal infringement of a copyright	18 U.S.C. § 2319
22	Criminal offenses [related to copyright]	17 U.S.C. § 506
23	Unauthorized publication or use of communications	47 U.S.C. 605
Procedural cybercrime laws		
24	Interception of wire, oral, or electronic communication	18 U.S.C. §§ 2510-2522
25	Preservation and disclosure of stored wire and electronic communication	18 U.S.C. §§ 2701-2712
26	Pen registers and trap and trace devices	18 U.S.C. §§ 3121-3127