Advances in Computer Science and Information Technology (ACSIT)
Print ISSN: 2393-9907; Online ISSN: 2393-9915; Volume 2, Number 1; January-March, 2015 pp. 71-76
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/acsit.html

Cyber Security: A Challenge for India

Ms. Shuchi Shukla

15th Year Student Of Integrated B.Tech(CSE)+MBA(Finance, HR) In Gautam Buddha University
E-mail: shuchi2810@gmail.com

Abstract—*This research paper is about the Cyber security which has been a challenge for world due to increase in number of cyber crimes every year. This research would be completed with the help of secondary resources. In this we would be studying about cyber crime , what cyber crime includes of (types of cyber crime),what are the initiative taken by Indian Government in this field to overcome the problem, what steps should be taken by individual so that they are not being webbed in the cyber crime network. The decrease in cyber crime will help the young generation most because all the cyber crime that has been convicted so far was found to be in age of 16-25.*

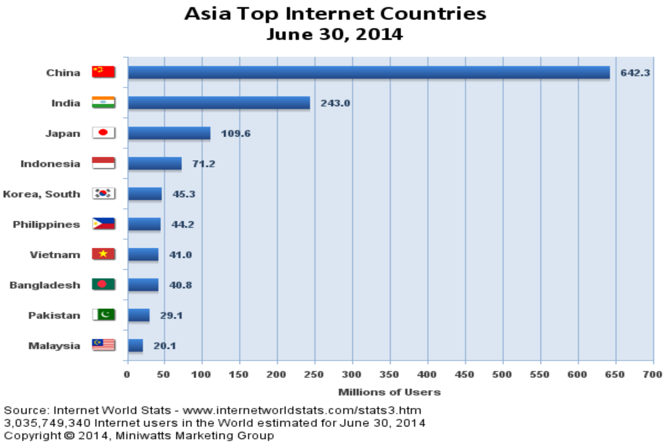
Keywords: *Cyber Crime, Phishing, Cyber law, Cyber cells, Cyber security*

1. INTRODUCTION

Internet is the world's largest networking system which facilitates every individual of the society or we can say it's the best way of circulating news ,data ,information and many more such technical help to the world's highest population. In other word we can say it has the solution to our every problem .Internet is now accepted globally or we can say its part of globalization. As we know everything comes with both pros and cons likewise internet also has its both pros and cons, likewise the number of users of internet is increasing on other hand number of cyber crime is also increasing. cyber crime has become a big challenge for the cyber security department. As per the data on the internet world stats website it was found that Asia has 45.7% of worlds total internet users, and around 243 million users are from India. [21].The Graph 1.1 shows us the statistics of Asian countries which depict us clearly about internet usage. India has the second largest number of Internet user among all the Asian countries.

It is expected that cyber crime is going to take a huge turn in 2015, cyber experts warned also that in upcoming times the fraudsters are gone take help of some new tricks to target the victims. Cyber Experts are accepting that fraudsters are going to target the organized sector more in order to be targeted, and planned some continuous attacks, which is known as APT (advanced persistent threats).This was the prediction which was made by Kaspersky Lab's Global Research and Analysis Team (GReAT).Since, 2008 every year it releases the list of cyber attack trends. [12]

GRAPH 1.1



Source: Internet World Stats - www.internetworldstats.com/stats3.htm
3,035,749,340 Internet users in the World estimated for June 30, 2014
Copyright © 2014, Miniwatts Marketing Group

Source: http://www.internetworldstats.com/stats3.htm#asia

2. WHAT IS CYBER CRIME?

The word "Cyber Crime" means the crime which is related to cyber web (related to computer and its world of internet). Cyber Crime includes all the illegal activities like accessing information through unauthorized sources, breaking up or stealing anyone's personal profile detail to login their accounts. It also includes the web crime which make people trap in some kind of financial activities and there are many crime related to cyber like virus attacks, financial crimes, sale of illegal articles, pornography, online gambling, e-mail spamming, cyber phishing, 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 Crime is being categorized in two parts :one is Cyber crime in which the computers are the target ,in such cyber crimes hackers hack the computers in order to corrupt the files or misuse the data and information. And on other hand crime or fraud which takes place with the help of computers.

In 2011 Dr. Debarati Halder and Dr. K. Jaishankar defines the cyber crime as "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)".

There are many researches and surveys which was conducted in regard of cyber crime and found that every two out of three persons who are being convicted for the cyber crime lies in the age group of 15 to 26 years because in this age group children don’t think twice before doing any wrong deed they just do things which they feel is right they don’t think the after circumstances of it.

3. TYPES OF CYBER CRIME

Credit/Debit Card Fraud: It is fraud which can be done when the user is using some unauthorized sight for transaction , at that time users personal details , card number and CVV number of the card can be traced for the further crime which can be made afterwards with the help of the details which has been stolen . So everyone before making payment online should be bit more careful so that they don’t get trapped in such deeds.

Computer Fraud: It is the cyber crime which has been convicted most rapidly in few years. Computer Fraud is the fraud which uses information technology to perform fraud; it is also termed as internet fraud. In this hackers (black hat hackers) take the help of internet and many activities linked with internet to commit the fraud or crime. It is a punishable offence.

Cyber Bullying: It is the type of cyber crime which is done intentionally to harm someone’s self respect or in other word to harass, embarrass or insult someone by using internet, email or any other electronic communication.

Cyber Stalking/Online harassment: It is done by hackers when the target is known sometimes and sometimes a random person, it harms the victim’s personal life as victim is continually bombarded with the mails and other type of electronic communication in order to get trapped or harass the victim, it sometime done to disturbed the person mentally or emotionally**.**

Malicious Programs/Viruses: In this viruses and malicious programs which harm the victim by harming there computer resources (like corrupting files or, crashing computer system, deleting some important data).Malicious programs are sub divided into 5 groups but all of them do the same work which is harming or infecting the computer software or hardware: Worms, Viruses, Trojans, Hacker utilities. Other malware .With the help of malicious programs the BotNet crimes also take place .This word is being derived from two different words: Robot and network. In this criminal take the control over the computer using malicious programs in order to make crime.

Online Child Pornography: Online Child pornography is the exploitation of children sexually with the help of illegal media that has been shared with the help of internet.

“Unfortunately, we´ve also seen a historic rise in the distribution of child pornography, in the number of images being shared online, and in the level of violence associated with child exploitation and sexual abuse crimes. Tragically, the only place we´ve seen a decrease is in the age of victims. This is – quite simply – unacceptable.”-Attorney General Eric Holder Jr. speaks at the National Strategy Conference on Combating Child Exploitation in San Jose, California, May 19, 2011.[14]

Unwanted exposure to sexually explicit material etc. It is a crime which is done intentionally by sending some unwanted clippings, pictures etc by email or some electronic media ,it also includes the video and pictures which has been saved while video chatting through webcam.

Hacking: Its is about stealing someone’s personal information (like login password ,id of facebook ,orkut or any such account, stealing some organizations detail) with the help of unwanted coding which is mostly done by black hat hackers.

Identity Theft: When the cyber crime takes place with the help of someone’s personal information without coming in the notice of that person. It is basically a tool with the help of which frauds take place; it is sometimes used to manipulate data’s and many fraud schemes

IP Spoofing: It is a technique in which hacker access to someone else computer by creating the image of trusted access, in which intruder sends the information from the trusted host IP address, in order to break the secure and trusted IP address hacker need to use various techniques in order to make modification in the packet headers so that packet appears to be coming from trusted host IP address.

Phishing: It is a technique in which fraudster tries to steal individuals personal information such as passwords, credit card and bank account number via emails and other electronic communication, in this victim is been provided with a hyperlinks with take victims to the fraud sites and after that fraud take place by providing showing golden world to user in order to con them. There is also one term known as Voice Phishing, in this fraudster copies someone’s voice in order to gain personal information.

Spam: It is the channel or technique the user of electronic mail services gets bulk of emails in which they have been provided with the best offers on the product and services. The main purpose of the such mail is to con user, if the user get trapped in the offer which they are providing, then before completing the deal they ask for the payment to be made, and once you made the payment or provide the information of your account or credit/debit card user is never going to receive further information from spammer, nor he is going to receive the product

Cyber terrorism: Cyber terrorism is a vast term if you ask 10 cyber experts you will almost get 8 different answer .The general meaning of cyber terrorism is a crime or terrorism who has adapted the computer as a source of threaten the victims by causing loss to them by attacking electronic resources like crashing the data, manipulation of information and much more.

Denning (2000) makes the following statement:

Cyber terrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber terrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.[19]

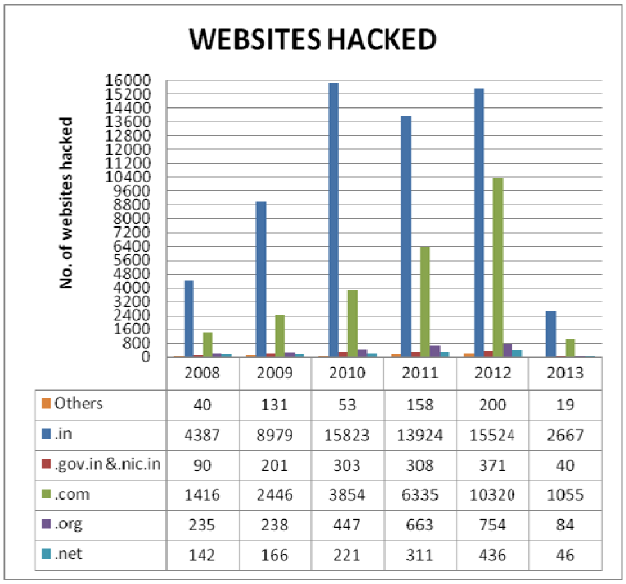
Internet Time Thefts: It is the type of hacking in which fraudster or hackers hacks some other person's ISP user ID and password and access the internet without the knowledge of that person and the particular person keeps on paying for the Internet Hours which he hasn't even used.

4. SCENARIO OF CYBER CRIME IN INDIA

Current scenario of cyber crime in India has been witnessed a significant increase in some past years .Many cyber attacks are done in which the targets are Government, public sector and private sector IT infrastructures in which they try to hack website,frauding,stealing information, phishing and many more . About 300 end user systems on an average are reported to be compromised on a daily basis. More than 100,000 viruses/worms variants are reported to be propagated on the net on a daily basis, of which 10,000 are new and unique. [3]This is according to **Standing Committee On Information Technology** 2012-13) this report was presented in lok sabha on 12th feburary,14.All data has been taken from this report only to make all the three graphs: Website hacked, cases registered and persons arrested.

The above graph 4.1 shows the number of sites status that is been hacked since 2008 to 2013.

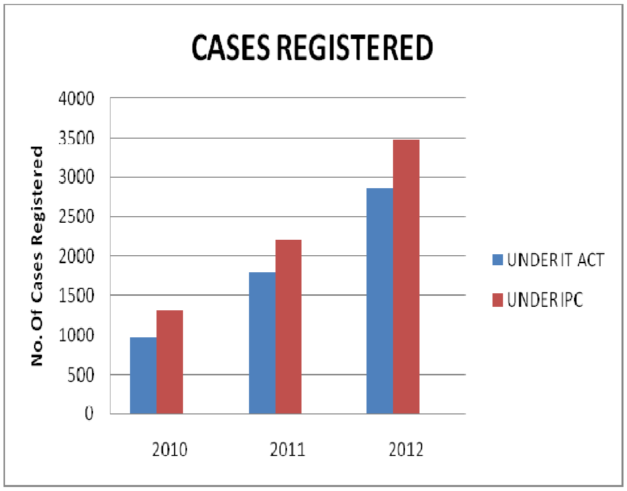
GRAPH 4.1



	2008	2009	2010	2011	2012	2013
🟧 Others	40	131	53	158	200	19
🟦 .in	4387	8979	15823	13924	15524	2667
🟥 .gov.in&.nic.in	90	201	303	308	371	40
🟩 .com	1416	2446	3854	6335	10320	1055
🟪 .org	235	238	447	663	754	84
🟦 .net	142	166	221	311	436	46

"During the years 2011, 2012, 2013 and 2014 (till May), a total number of 21,699, 27,605, 28,481 and 9,174 Indian websites were hacked by various hacker groups spread across worldwide. In addition, during these years, a total number of 13,301, 22,060, 71,780 and 62,189 security incidents, respectively, were reported to the CERT-In," Said by Ravi Shankar Prasad, Communication and IT minister.[18]

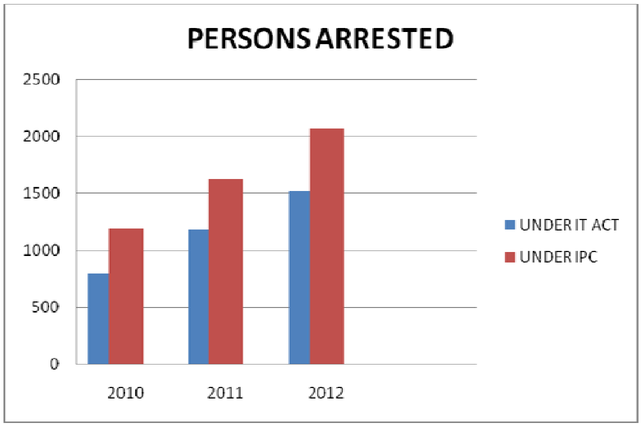
GRAPH 4.2



The graph 4.2 depicts the cases registered in three years: 2010, 2011 and 2012 under IT act and under IPC act.

These two acts are made by government of India to govern and the check the cyber crime that is increasing tremendously, these acts are made to control and punish the persons under these acts .The graph 4.3 shows the number of person arrested in 3 years under these act out of total case registered.

GRAPH 4.3



5. CYBER CRIME PREVENTION: ROLE OF CERT-IN

CERT-IN is the Indian Computer Experts Response Team involves the group of experts who handle or immediate ready to respond to any problem that is being raised against the cyber security of the country and also perform service quality management services**.** It is the Government organization which comes under Technology. Some main role of CERT-In preventing cyber attacks are:-

- ✓ It coordinates the responses to the security incidents that take make and also respond to the major events.
- ✓ It is an advisory which give advices on Issues related to cyber crime and gives timely warnings regarding imminent threats.
- ✓ It work which the security experts on industry , government and many more to identify the optimum solution for all the security problems.
- ✓ It helps in Analyzing the vulnerabilities of the product and its malicious code
- ✓ It helps in Analysizing the web defacements on regular basis
- ✓ It helps organizations to mitigate spams and anomous threats.
- ✓ It help many organizations: public and private both in profiling the network and then attacking systems
- ✓ Interact with vendors and others at large to provide effective and timely solutions for incident resolution and investigation
- ✓ It Conduct training programs on specialized topics of cyber security to create awareness among the peoples
- ✓ It Develop security guidelines in order to protect people from cyber crime.
- ✓ It is Collaborating with Industry so that we can have some effective incident resolution

6. POLICY INITIATIVES

6.1. CCMP (Cyber Crisis Management Plan)

It is the initiative which government of India takes in order to manage the cyber crime. So that we are able to identify the cyber risk and threats easily and after identifying we are able to deal with it by avoiding it or taking some steps in order to reduce it and manage it. In different organizations we have crisis management department, in which cyber experts are there to manage and portfolio the risk.

6.2. National Cyber Security Policy, 2013 (NCSP-2013)

National Cyber Security Policy(NCSP)) is the policy which has been framed by DeitY(Department of Electronics and Information Technology), Ministry of Communication and Information Technology, (GOI)Government of India. The main focus of this policy is to protect or govern the public and private IT infrastructure from the cyber crime, and also to save the information from the fraudsters .But the policies wasn't able to come up to the expectations, it was suffering the various drawbacks .It was found that after the declaration of the policy it doesn't came into the force till 21st November 2014.To overcome this problem The new policy Initiative took place which was named as NCCC(National Cyber Coordinate Center)

National Cyber Coordination Centre proposed the cyber security and e-surveillance agency in India. It basically includes the prevention strategies to the cyber crime, provide training to the cyber crime investigation and also review some old and outdated cyber laws. In order to protect the number of cyber crimes in the country.

6.3. Information Technology Act, 2000 and Cyber Security

The Information Technology Act 2000 (also known as ITA-2000 or the IT Act) is an Act of the Indian Parliament (No 21 of 2000) which came in the assistant of president of India on 9th June 2000 and in the same year on October 17, 2000 it came into force.

The act demanded for the legal provision for the e-transaction to facilitate electronic filling of documents with governments' agencies which involves many paper work and storage of information. This law is applied all kind of data information which is used in the context of commercial activities.

The main purpose of this act was to get legally recognized for the transaction purpose in which digital signature should get authentification under the law .But due to some drawback this act was not able to come up to the expectations and not been able to solve the problem for which it was made. So after that in 2008 the first legislation for Information and Communication technology was made which was known as ITAA-2008(Information Technology Amendment Act 2008).It came into the presidents assistance on 5th Feb 2009 and came into force on 27th October 2009.It covered all the drawbacks of the IT Act-2000.It gave recoginzation to e transaction, and also take care of the data privacy and many more.

7. CYBER CELLS

There are currently 21 cities in India in which cyber cells are working as per the updated list from Information Security Awareness program by Department of Electronics and Information Technology, Government of India till 8th January 2015.The list cities are given below

Table 7.1

S. No	Name Of Cities Have Working Cyber Cells
1	Assam
2	Bangalore
3	Bihar
4	Chennai
5	Delhi
6	Gujarat
7	Haryana
8	Himachal Pradesh
9	Hyderabad
10	Jammu
11	Jharkhand
12	Kerala
13	Meghalaya
14	Mumbai
15	Orissa
16	Pune
17	Punjab
18	Thane
19	Uttarakhand
20	Uttar Pradesh
21	West Bengal

Source: http://infosecawareness.in/cyber-crime-cells-in-india this is updated list till 8th Jan 2015

8. PREVENTION INDIVIDUAL SHOULD TAKE IN ORDER TO PROTECT HIMSELF/HERSELF FROM THE CYBER WEB TRAP.

Some steps and practices that can help one to minimize risk of being trapped in web of cyber crime:

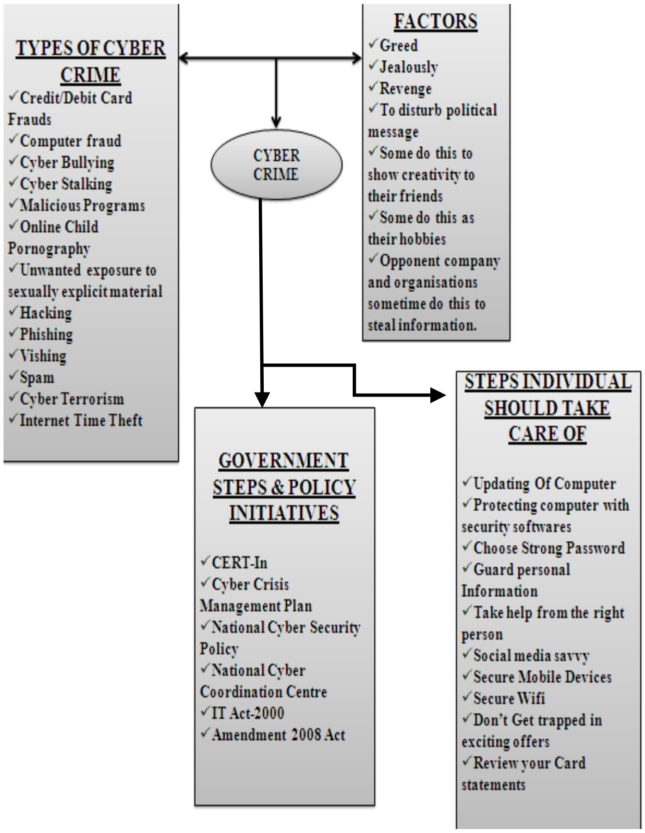
Updating of Computer Systems This step avoid the cyber attack and in this we make sure that are system are up to date means it is fully equipped with all the updated software ,latest antivirus. But it doesn't make sure that your system is cent percent safe .However, it make difficult for hackers to access the system.

Protecting computer with security software Security software is that software which helps to guard computer from malicious programs. Security software basically includes ant viruses and firewall.

Choosing strong passwords Password is the way to secure your account or data, so always select the strong password .Avoid the password which is common or can be easily be hacked by hackers. Always choose the password which is the combination of lowercase, uppercase, numbers and special characters .And make the habit of changing password very frequently.

Guard/Protect Personal Information In order to take advantage from any online site you need to provide your personal details. So in that case guard your personal information one should be very careful while taking advantage of such services, it should only be done from trusted sites. Phishing mails should be avoided, don't respond to unknown mails and tell the personal information to them, guard your email with the spammers.

9. PROPOSED MODEL


TYPES OF CYBER CRIME
✓Credit/Debit Card Frauds
✓Computer fraud
✓Cyber Bullying
✓Cyber Stalking
✓Malicious Programs
✓Online Child Pornography
✓Unwanted exposure to sexually explicit material
✓Hacking
✓Phishing
✓Vishing
✓Spam
✓Cyber Terrorism
✓Internet Time Theft
FACTORS
✓Greed
✓Jealously
✓Revenge
✓To disturb political message
✓Some do this to show creativity to their friends
✓Some do this as their hobbies
✓Opponent company and organisations sometime do this to steal information.
CYBER CRIME
GOVERNMENT STEPS & POLICY INITIATIVES
✓CERT-In
✓Cyber Crisis Management Plan
✓National Cyber Security Policy
✓National Cyber Coordination Centre
✓IT Act-2000
✓Amendment 2008 Act
STEPS INDIVIDUAL SHOULD TAKE CARE OF
✓Updating Of Computer
✓Protecting computer with security softwares
✓Choose Strong Password
✓Guard personal Information
✓Take help from the right person
✓Social media savvy
✓Secure Mobile Devices
✓Secure Wifi
✓Don't Get trapped in exciting offers
✓Review your Card statements

Take the help from right person If some kind of repair or assistance is needed to rectify the computer problem like maintenance or software updating then computer technician called for the help should be authenticated service provider or a certified computer technician. So that there is no threat to your data.

Social-Media Savvy The social media profile should be set to the privacy setting and review the security setting at frequent interval of time

Secure Mobile Devices & Secure wireless network mobile devices and the wireless networks at home are more vulnerable if they are not properly secure. So while downloading applications in mobile be aware and choose trusted source

10. CONCLUSION

Internet and communication Technology is influencing everyone's life in one or another way. In comparison to all other developing countries it was found that India has 243 millions internet user .As number of cyber usage is increasing in the same way number of cyber crime is also increasing. It has been seen that most of the cyber crimes that takes place is done by young generation .This study review us about the criminal offence that take place with the help of computer .It tells us about the websites that is been hacked in some past years .We can draw that the result about the various schemes, practices and the awareness program that can help an individual, organization to beware of the cyber crimes. In this research we have analyzed the steps that an individual should take care of in order to protect himself/herself from the fraudsters .In the upcoming time Information security teams would requires more number of skilled experts to deal with the different type of the cyber attackers. Every individual should be more careful at the time of dealing with any type of online transaction or while telling your personal information to someone.

Nowadays cybercrime has become a global issue which need to be resolved, therefore many laws has been enforced by different agencies including State police to collaborate with the CBI(Central Bureau of Investigation),NTRO(National Technical Research Organization) , Cert-In (Computer Experts Response Team-Indian) and INTERPOL to reduce number of cyber crimes.

REFERENCES

[1] Crime in India: 2011-Compendium (2012), National Crime Records Bureau, Ministry of Home Affairs, Government of India,New Delhi, India.

[2] Cyber Law & Information Technology (2011) by Talwant Singh, Additional District & Sessions Judge, New Delhi, India.

[3] Fifteenth Lokha Sabha , Fifty-Second Report, Standing Committee On Information Technology (2013-14),Ministry Of Communications And Information Technology (Department Of Electronics And Information Technology) Cyber Crime, Cyber Security And Right To Privacy

[4] Godbole & Belapure ,Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley India Pvt. Ltd, New Delhi, India,2012.

[5] Haldaer & JaishankarCyber Crime and the Victimization of Women: Laws, Rights and Regulations ,IGI Global, USA,2011.

[6] [6] Muthukumaran ,"Cyber Crime Scenario In India", Criminal Investigation Department Review,Januaray 2008

[7] Nagpal,Introduction to Indian Cyber Law , Asian School of Cyber Laws, Pune, India,2008.

[8] Seth,Cyber Laws in the Information Technology Age , Jain Book Depot, New Delhi, India,2009.

[9] Shrivastav& Ekata," ICT Penetration and Cybercrime in India: A Review", International Journal Of Advanced Research In Computer Science and Software Engineering, Volume 3 ,Issue 7,July 2013

[10] *Singh & Kandpal* ,"Latest Face of Cybercrime and Its Prevention In India",International Journal Of Basics And Applied Sciences,Vol 2 No. 4

[11] Suri & Chhabra, Cyber Crime ,Pentagon Press, New Delhi, India,2003.

[12] TimesofIndia,http://timesofindia.indiatimes.com/city/nagpur/Cyber-criminals-will-be-more-persistent-elusive-in-2015/articleshow/45754409.cms

[13] http://infosecawareness.in/cyber-crime-cells-in-india

[14] http://www.justice.gov/criminal/ceos/subjectareas/childporn.html

[15] http://www.philstar.com/business/2013/03/12/918801/study-social-networks-new-haven-cybercrime

[16] http://www.symantec.com/en/in/about/news/release/article.jsp?prid=20130428_01

[17] http://en.wikipedia.org/wiki/Computer_crime

[18] http://www.livemint.com/Politics/NNuFBA3F2iX4kxIXqKaX2K/CERTIn-reports-over-62000-cyber-attacks-till-May-2014.html?utm_source=copy

[19] http://www.symantec.com/avcenter/reference/cyberterrorism.pdf

[20] http://www.crime-research.org/library/Cyber-terrorism.htm

[21] http://www.internetworldstats.com/stats3.htm#asia