Present Cyber Crime Scenario & Prevention Measures in India

Prof. Shreyas Upendra Dingankar
IMED, Bharati Vidyapeeth Pune

Abstract:

Cyber crime is emerging as a serious threat. Worldwide governments, police departments and intelligence units have started to react. Initiatives to curb cross border cyber threats are taking shape. Indian police has initiated special cyber cells across the country and have started educating the personnel. This article is an attempt to provide a glimpse on cyber crime in India. This article is based on secondary data sources like various reports from news media and news portal. The paper also includes Indian cybercrime Statistics, cyber crime cells all over India and many more latest news. National level agencies can develop security guidelines and policy to prevent and safeguard of internet users from cyber crimes.

Introduction:

1. What is Cybercrime?

Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets, or use the Internet for exploitive or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers.

Cybercrime may also be referred to as computer crime.

2. Cyber Crimes Includes

Following are the few examples of cybercrime:

Types of cyber crimes:

1. Hat Hackers
2. Grey Hat Hackers
3. Cyber Stalking
4. Hacking White & Black Spamming
5. Cyber Pornography
6. Phishing
7. Software Piracy
8. Password Sniffers
9. Spoofing
10. Credit Card Fraud
11. Web Jacking
12. Cyber terrorism
13. Email Bombing

Keywords

Cybercrime, prevention, cyber cases, hacking and cyber cells in India, Indian cyber-crime statistics, cyber-attack

2.1 Hat Hackers:

The definition of the word "hacker" is controversial, and could mean either someone who compromises computer security or a skilled developer in the free software or open-source movements.

Hackers aren't inherently bad — the word "hacker" doesn't mean "criminal" or "bad guy." Geeks and tech writers often refer to "black hat," "white hat," and "gray hat" hackers. These terms define different groups of hackers based on their behavior.

2.2 Gray Hats:

Very few things in life are clear black-and-white categories. In reality, there's often a gray area. A gray-hat hacker falls somewhere between a black hat and a white hat. A gray hat doesn't work for their own personal gain or to cause carnage, but they may technically commit crimes and do arguably unethical things.

For example, a black hat hacker would compromise a computer system without permission, stealing the data inside for their own personal gain or vandalizing the system. A white-hat hacker would ask for permission before testing the system's security and alert the organization after compromising it. A gray-hat hacker might attempt to compromise a computer system without permission, informing the organization after the fact and allowing them to fix the problem. While the gray-hat hacker didn't use their access for bad purposes, they compromised a security system without permission, which is illegal.

If a gray-hat hacker discovers a security flaw in a piece of software or on a website, they may disclose the flaw publically instead of privately disclosing the flaw to the organization and giving them time to fix it. They wouldn't take advantage of the flaw for their own personal gain — that would be black-hat behavior — but the public disclosure could cause carnage as black-hat hackers tried to take advantage of the flaw before it was fixed.

2.3 Cyberstalking :

Cyber stalking is a crime in which the attacker harasses a victim using electronic communication, such as e-mail or instant messaging (IM), or messages posted to a Web site or a discussion group. A cyber stalker relies upon the anonymity afforded by the Internet to allow them to stalk their victim without being detected.

Cyber Stalking

2.4 Black Hat:

Just like in the old westerns, these are the bad guys. A black hat is a cracker. To add insult to injury, black hats may also share information about the "break in" with other black hat crackers so they can exploit the same vulnerabilities before the victim becomes aware and takes appropriate measures… like calling Global Digital Forensics!

2.5 White hat:

describes a hacker (or, if you prefer, cracker) who identifies a security weakness in a computer system or network but, instead of taking malicious advantage of it, exposes the weakness in a way that will allow the system's owners to fix the breach before it can be taken advantage by others (such as black hat hackers.) Methods of telling the owners about it range from a simple phone call through sending an e-mail note to a Webmaster or administrator all the way to leaving an electronic "calling card" in the system that makes it obvious that security has been breached.

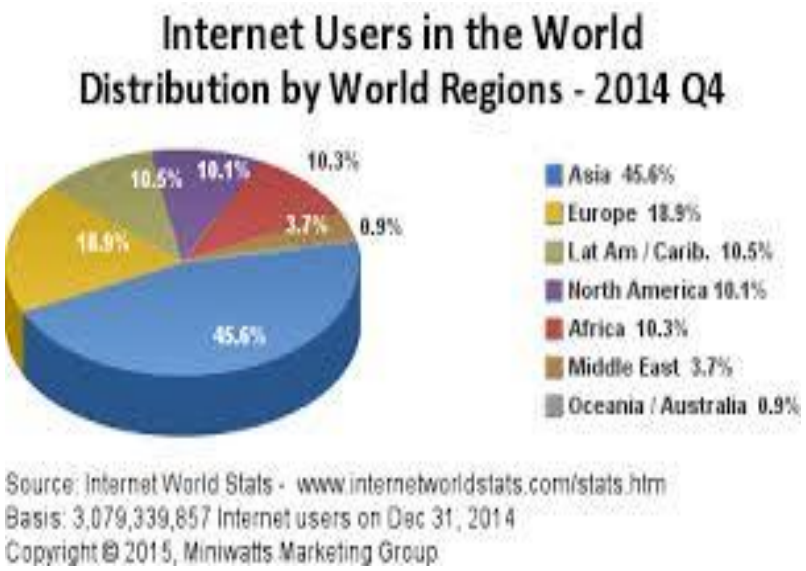
3. Malicious Software:

*These are Internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to steal sensitive information or data or causing damage to software present in the system***.**

4. Current Scenario:

These days computers and internet has become very Necessary and useful for our daily life. Today the internet is the great mediator of our lives. Today people can get information, store information and share information through the internet. Almost 20-25 years back there were 125000 people users who used internet but now around 60, 00, 00,000 people are surfing the net around the globe. The fastest growing world of internet is known as cyber world. Today cyber world are fastest moving and high technology world. Asian countries are mostly Internet Users in world.

In Asia region India has rank top two internet users country, so India is the very fastest growing country. Today internet becomes the backbone of social & economic world. Users can access the internet anytime from anywhere but through the internet many illegal works may done. Today E-mail and website is the most efficient way of data communication.



Objectives:

1. **To Study the Concept Of cyber Crime –**

   Cyber laws in India

   In INDIA information technology act 2000 deals with the cybercrime activities /problems. It act 2000 has both positive and negative aspects as well. Therefore amendment is done in Rajya Sabha on Dec 23rd of 2008.this act was renamed as information technology(Amendment) act 2008 and referred as ITAA 2008.

   Penalties for Damage to Computer System

   According to Section: 43 of 'Information Technology Act 2000', If any person without permission of the owner or any other person who is in charge of a computer, -accesses or uses a computer system or disrupts, degrades, or causes disruption to intension of damaging whole data then a person shall be punishable. If there is any failure in protecting the data/ information then a company which provides protection shall be liable to pay compensation to victims.

2. **To Analyse the Report related to Cyber Crime:**

   Those who attempt to predict the future run the risk of being wrong. But those who overlook the importance of conducting a prospective analysis adopt a passive attitude that weakens them against the dictatorship of events. Anticipating societal changes prepares us to weather the storm. The pioneers of the Internet, including the recently deceased Paul Baran, certainly never imagined that the Internet would connect more than two billion subscribers half a century later. Who could have predicted it?

   The boom in digital technology is changing the foundation of our society. Who would have imagined its impact on telecommunications, social relationships, the economy, industrial processes, home automation, politics, and countless other areas? Some compare the digital revolution to Gutenberg's invention of the printing press. Surely, the change has even greater magnitude, because it touches all human activities. Each and every day, we bear witness to a true reconfiguration that affects individuals, businesses, and institutions.

Cyberspace is a place of freedom, creativity, and growth, with "exponential" prospects. It is a chance for humanity. Yet all progress has its downside.

The perverse effects manifest themselves as well, as predators immediately exploit vulnerabilities in order to gain profits, destroying or neutralising anything that stands in the way of expanding their criminal enterprise. Cyberspace promises opportunities, but it is also grounds for power and conflict. It's war! We can imagine a future based on certainty. Cyberspace will link more and more people together, in developed countries and even more so in emerging countries, particularly China. This expansion can also be seen in third-world countries, which now have access to new technologies, by making a quantum leap that blurs stinging differences. New technologies will also enrich daily life down to the finest detail. That is another certainty. The notion of power will have to be examined in a new light, and the expression of democracy will break free from the schedule of electoral consultations. Public and private institutions will have to adapt to this new citizens and consumers behaviour. Organizational methods will shift toward a more complex matrix system. Those in charge must identify the things that will remain the same and also detect potential breakthroughs in changing technologies. Hence the importance of scientific monitoring.

The future also depends on uncertainties. Will countries, whose legitimacy resides primarily in defence and security, be able to maintain such a monopoly when faced with multiple daily threats or attacks that may come without warning and from various sources? Will international cooperation be able to overcome the contradiction between an inherent globalization of networks and the maintenance of political, legal and military borders? Can the measures that need to be taken for defence and security receive funding during the prolonged economic crisis, measures that are needed to supplement – not replace – those that are already needed in order to guarantee peace in the air and at sea? Will "black" countries, mafias, criminal organizations, and terrorist movements reap the benefits of free actions and resources that may be lacking among those who seek to prevent their empire from growing? Building awareness is paramount if we want to avoid chaos. Governments are committed to this today with resolution.

3. To suggest measures of Protection to people from Cyber Crime:

1. **Use Strong Passwords**
   Use different user ID / password combinations for different accounts and avoid writing them down. Make the passwords more complicated by combining letters, numbers, special characters (minimum 10 characters in total) and change them on a regular basis.

2. **Secure your computer**

   a. **Activate your firewall**
      Firewalls are the first line of cyber defense; they block connections to unknown or bogus sites and will keep out some types of viruses and hackers.

   b. **Use anti-virus/malware software**
      Prevent viruses from infecting your computer by installing and regularly updating anti-virus software.

c. **Block spyware attacks**
Prevent spyware from infiltrating your computer by installing and updating anti-spyware software.

3. **Be Social-Media Savvy**
Make sure your social networking profiles (e.g. Facebook, Twitter, Youtube, MSN, etc.) are set to private. Check your security settings. Be careful what information you post online. Once it is on the Internet, it is there forever!

4. **Secure your Mobile Devices**
Be aware that your mobile device is vulnerable to viruses and hackers. Download applications from trusted sources.

5. **Install the latest operating system updates**
Keep your applications and operating system (e.g. Windows, Mac, Linux) current with the latest system updates. Turn on automatic updates to prevent potential attacks on older software.

6. **Protect your Data**
Use encryption for your most sensitive files such as tax returns or financial records, make regular back-ups of all your important data, and store it in another location.

7. **Secure your wireless network**
Wi-Fi (wireless) networks at home are vulnerable to intrusion if they are not properly secured. Review and modify default settings. Public Wi-Fi, a.k.a. “Hot Spots”, are also vulnerable. Avoid conducting financial or corporate transactions on these networks.

8. **Protect your e-identity**
Be cautious when giving out personal information such as your name, address, phone number or financial information on the Internet. Make sure that websites are secure (e.g. when making online purchases) or that you’ve enabled privacy settings (e.g. when accessing/using social networking sites).

9. **Avoid being scammed**
Always think before you click on a link or file of unknown origin. Don’t feel pressured by any emails. Check the source of the message. When in doubt, verify the source. Never reply to emails that ask you to verify your information or confirm your user ID or password.

10. **Call the right person for help**
Don’t panic! If you are a victim, if you encounter illegal Internet content (e.g. child exploitation) or if you suspect a computer crime, identity theft or a commercial scam, report this to your local police. If you need help with maintenance or software installation on your computer, consult with your service provider or a certified computer technician.

- **Methodology**

Cyber warfare:

It is Internet-based conflict involving politically motivated attacks on information systems. Cyber warfare attacks can disable official websites and networks, disrupt or disable essential services, steal or alter classified data, and cripple financial systems -- among many other possibilities.

Domain hijacking:

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

SMS Spoofing:

SMS spoofing is a relatively new technology which uses the short message service (SMS), available on most mobile phones and personal digital assistants, to set who the message appears to come from by replacing the originating mobile number (Sender ID) with alphanumeric text. Spoofing has both legitimate uses (setting the company name from which the message is being sent, setting your own mobile number, or a product name) and illegitimate uses (such as impersonating another person, company, and product).

Voice Phishing:

The term is a combination of "voice" and phishing. Voice phishing is use to gain access of private, personal and financial information from the public. Voice phishing uses a landline telephone call to get information.

Cyber trafficking:

It may be trafficking in weapons, drugs, human beings, which affect the large numbers of persons.

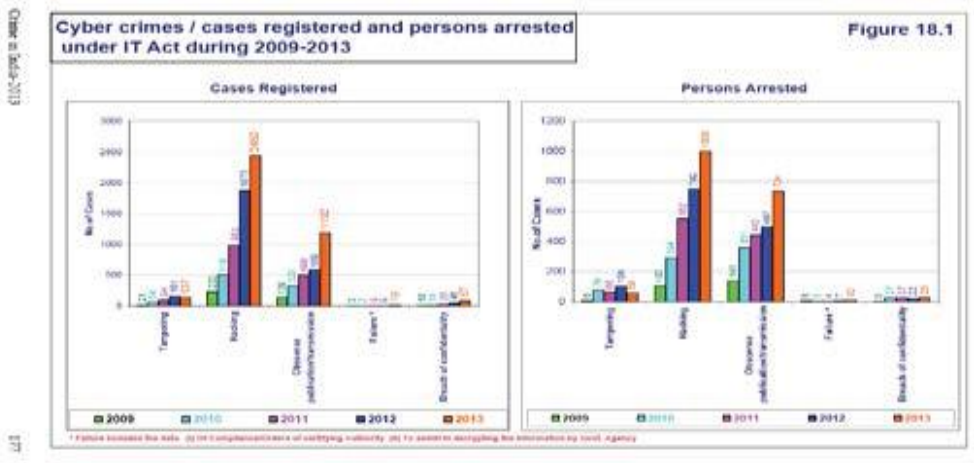
Present trends of Cybercrime in India

India is trying to implement the Digital India poor track record project to the best of its capabilities. The success of Digital India project would depend upon maximum connectivity with minimum cyber security risks. This is also a problem for India as India has a of cyber security. According to Home Ministry statistics, as many as 71,780 cyber frauds were reported in 2013, while 22,060 such cases were reported in 2012. There have been 62,189 incidents of cyber frauds till June 2014.

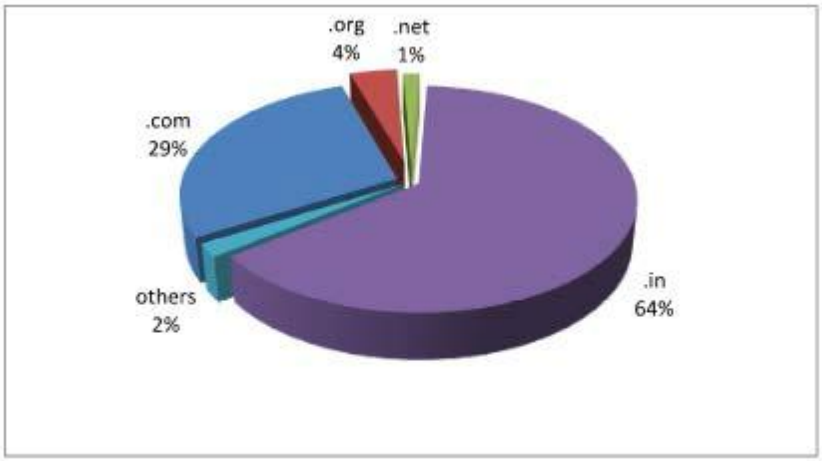
In 2013, a total of 28,481 Indian websites were hacked by various hacker groups spread across the globe. The numbers of hacking incidents were 27,605 in 2012 and 21,699 in 2011.
As per the cyber-crime data maintained by National Cyber Records Bureau, a total of 1,791, 2,876 and 4,356 cases were registered under the Information Technology Act in 2011, 2012

and 2013, respectively. A total of 422, 601 and 1,337 cases were registered under cyber-crime related sections of the Indian Penal Code in 2011, 2012 and 2013, respectively.

There has been an annual increase of more than 40 per cent in cyber-crime cases registered in the country during the past two-three years,



According National Crime Records Bureau (NCRB), a total of 288, 420, 966, 1,791 and 2,876 cyber-crime cases were registered under IT Act during 2008, 2009, 2010, 2011 and 2012, respectively. As per the information reported to and tracked by Indian Computer Response Team (CERT-In), a total number of 308, 371 and 78 government websites were hacked during the years 2011, 2012 and 2013 respectively and 16,035 incidents related to spam, malware infection and system break-in were reported in 2013.



Statistics of case registered and people arrested under Indian IPC Section and IT Act

Year	Under Indian IPC Sections		Under Indian IT ACT	
	Cases registered	People arrest	Cases registered	People arrest
2009	276	263	420	228
2010	356	394	966	779
2011	422	446	1791	1184
2012	601	549	2876	1522

(Source: Crime in India- 2012, Compendium, National Crime Records Bureau Ministry of Home Affairs Government of India)

Cybercrime Prevention Strategies

More recent versions of Cybercrime is considered one the most dangerous threats for the development of any state; it has a serious impact on every aspect of the growth of a country. Government entities, non-profit organizations, private companies and citizens are all potential targets of the cyber criminal syndicate. Cyber criminals are no different than traditional criminals in that they want to make their money as quickly and easily as possible. Cybercrime prevention can be achieved fairly quickly and in a cost-effective manner the prevention of cyber criminal activities is the most critical aspect in the fight against cybercrime. It's mainly based on the concepts of awareness and information sharing. A proper security posture is the best defense against cybercrime. Every single user of technology must be aware of the risks of exposure to cyber threats, and should be educated about the best practices to adopt in order to reduce their "attack surface" and mitigate the risks.

Awarness:

Best Practices for Prevention of Cybercrime

1. Below mentioned security guidelines and good practices may be followed to minimize the security risk of cybercrime:
   By updating the computers: keep your computer current with the latest patches and updates. One of the best ways to keep attackers away from your computer is to apply patches and other software fixes when they become available. By regularly updating your computer, you block attackers from being able to take advantage of software flaws (vulnerabilities) that they could otherwise use to break into your system. While keeping your computer up-to-date will not protect you from all attacks, it makes it much more difficult for hackers to gain access to your system, blocks many basic and automated attacks completely, and might be enough to discourage a less-determined attacker to look for a more vulnerable computer elsewhere. choose strong passwords and keep them safe passwords are a fact of life on the internet today—we use them for everything from ordering flowers and online banking to logging into our favorite airline Web site to see how many miles we have accumulated. The following tips can help make your online experiences secure

2. Selecting a password that cannot be easily guessed is the first step toward keeping passwords secure and away from the wrong hands. Strong passwords have eight characters or more and use a combination of letters, numbers and symbols (e.g. # $ %!?). Avoid using

any of the following as your password: your login name, anything based on your personal information such as your last name, and words that can be found in the dictionary. Try to select especially strong, unique passwords for protecting activities like online banking.

3. Keep your passwords in a safe place and try not to use the same password for every service you use online.

4. Change passwords on a regular basis, at least every 90 days. This can limit the damage caused by someone who has already gained access to your account. If you notice something suspicious with one of your online accounts, one of the first steps you can take is to change your password.

5. Protect your computer with security software: Several types of security software are necessary for basic online security. Security software essentials include firewall and antivirus programs. A firewall is usually your computer's first line of defense-it controls who and what can communicate with your computer online. You could think of a firewall as a sort of "policeman" that watches all the data attempting to flow in and out of your computer on the Internet, allowing communications that it knows are safe and blocking "bad" traffic such as attacks from ever reaching your computer. The next line of defense many times is your antivirus software, which monitors all online activities such as email messages and Web browsing and protects an individual from viruses, worms, Trojan horse and other type's malicious programs. More recent versions of antivirus programs, such as Norton Antivirus, also protect from spyware and potentially unwanted programs such as adware. Having security software that gives you control over software you may not want and protects you from online threats is essential to staying safe on the Internet. Your antivirus and antispyware software should be configured to update itself, and it should do so every time you connect to the Internet. Integrated security suites such as Norton Internet Security combine firewall, antivirus, antispyware with other features such as antispam and parental controls have become popular as they offer all the security software needed for online protection in a single package. Many people find using a security suite an attractive alternative to installing and configuring several different types of security software as well as keeping them all up-to-date.

6. Protect your personal information: Exercise caution when sharing personal information such as your name, home address, phone number, and email address online. To take advantage of many online services, you will inevitably have to provide personal information in order to handle billing and shipping of purchased goods. Since not divulging any personal information is rarely possible, the following list contains some advice for how to share personal information safely online:

7. Keep an eye out for phony email messages. Things that indicate a message may be fraudulent are misspellings, poor grammar, odd phrasings, Web site addresses with strange extensions, Web site addresses that are entirely numbers where there are normally words, and anything else out of the ordinary. Additionally, phishing messages will often tell you that you have to act quickly to keep your account open, update your security, or urge you to provide information immediately or else something bad will happen. Don't take the bait.

8. Don't respond to email messages that ask for personal information. Legitimate companies will not use email messages to ask for your personal information. When in doubt, contact the company by phone or by typing in the company Web address into your Web browser. Don't click on the links in these messages as they make take you to fraudulent, malicious Web sites.

9. Pay attention to privacy policies on Web sites and in software. It is important to understand how an organization might collect and use your personal information before you share it with them.

10. Guard your email address. Spammers and phishes sometimes send millions of messages to email addresses that may or may not exist in hopes of finding a potential victim. Responding to these messages or even downloading images ensures you will be added to their lists for more of the same messages in the future. Also be careful when posting your email address online in newsgroups, blogs or online communities.

11. Online offers that look too good to be true usually are. The old saying "there's no such thing as a free lunch" still rings true today. Supposedly "free" software such as screen savers or smiley's, secret investment tricks sure to make you untold fortunes, and contests that you've surprisingly won without entering are the enticing hooks used by companies to grab your attention.

12. Review bank and credit card statements regularly: The impact of identity theft and online crimes can be greatly reduced infuser can catch it shortly after their data is stolen or when user gets symptoms. Regularly check bank and credit card's statements. Now, many banks and services use fraud prevention systems that call out unusual purchasing behavior.

CONCLUSION:

It is cleared from the previous studies and records that with the increment in technology cybercrimes increases. Qualified people commit crime more so, there is need to know about principles and computer ethics for their use in proper manner. Cybercrime and hacking is not going away, if anything it is getting stronger. By studying past incidents, we can learn from them and use that information to prevent future crime. Cyber law will need to change and evolve as quickly as hackers do if it has any hopes of controlling cybercrime. Law must also find a balance between protecting citizens from crime, and infringing on their rights. The great thing about the internet is how vast and free it is. Will it be able to remain the same way while becoming tougher on criminals? Only time will tell. There will always be new and unexpected challenges to stay ahead of cyber criminals and cyber terrorists but we can win only through partnership and collaboration of both individuals and government. There is much we can do to ensure a safe, secure and trustworthy computing environment. It is crucial not only to our national sense of well-being, but also to our national security and economy. Yet India has taken a lot of steps to

stop cybercrime but the cyber law cannot afford to be static, it has to change with the changing time.

Suggestion:

We can arrange workshops, free advertisements, public interest with the help of government & NGO'S. The process of acknowledgment about cyber world crimes and cyber illiteracy should be start from grassroots level; institutes, computer centers, schools & individuals.

Reference:

- Crime in India: 2011-Compendium (2012), National Crime Records Bureau, Ministry of Home Affairs, Government of India,

New Delhi, India.

- Cyber Law & Information Technology (2011) by Talwant Singh, Additional District & Sessions Judge, New Delhi, India.
- Introduction to Indian Cyber Law (2008) by Rohas Nagpal, Asian School of Cyber Laws, Pune, India
- Cyber Crime (2003) by R.K. Suri and T.N. Chhabra, Pentagon Press, New Delhi, India.
- International Journal of Basic and Applied Sciences Kandpal & Singh Vol. 2. No.4 ISSN: 2277-1921.
- Cyber Laws in the Information Technology Age (2009) by Karnika Seth, Jain Book Depot, New Delhi, India.
- Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives (2012) by Nina Godbole and Sunil Belapure, Wiley India Pvt. Ltd, New Delhi, India.
- Cyber Crime and the Victimization of Women: Laws, Rights and Regulations (2011) by Debarati Haldaer (Centre for Cyber Victim Counseling, India) and K. Jaishankar (Manonmaniam Sundaranar University, India), IGI Global, USA.
- http://www.philstar.com/business/2013/03/12/918801/study-social-networks-new-haven-cybercrime
- http://www.symantec.com/en/in/about/news/release/article.jsp?prid=20130428_01
- http://www.internetworldstats.com/stats.htm
- http://en.wikipedia.org/wiki/Computer_crime

- Vineet Kandpal and R. K. Singh

MCA Student, IGNOU, New Delhi.
Scientist-D (Information Technology),
G. B. Pant Institute of Himalayan Environment and Development,
Kosi- Katarmal, Almora – 263643, Uttarakhand, India

- Prof .Sachin Ayarekar

Bharati Vidyapeeth Imed Pune