Present scenario of cybercrime in INDIA and its preventions

*Shubham Kumar,
*Engineering Student, CSE
Dronacharya College of Engineering

Guide Faculty - Dr.Santanu Koley, Associate Professor,
Dronacharya College of Engineering, UP, India
Email-santanukoley@yahoo.com

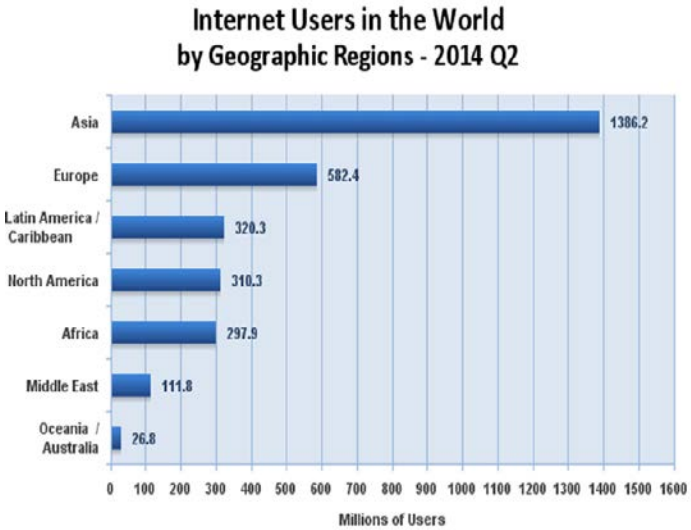
*Uday Kumar
*Engineering Student, CSE
Dronacharya College of Engineering

Abstract : The internet in India is growing rapidly. It has given rise to new opportunity in every field like – entertainment, business, sports, education etc. It is universally true that every coin has 2 sides, same for the internet, it uses has both advantage and disadvantage, and one of the most disadvantage is Cyber-crime. We can say, cyber-crime is any illegal activity which is committed using a computer network (especially the internet). Also, cyber-crime involves the breakdown of privacy, or damage to the computer system properties such as files, website pages or software. In India most of cyber-crime cases are committed by educated person (some cyber – crime requires skills). So, it is required the deep knowledge about the cyber –crime and it prevention. Also, in India most of the cases found where, crimes are committed due to lack of knowledge or by mistake. In this paper, I have discussed various categories and cases of cyber-crime which is committed due to lack of knowledge or sometimes due to intention behind. I also, suggested various preventive measures against these unlawful acts in day to day life.

Keywords: cybercrime, prevention, cyber cases, hacking, cyber cells in India, Indian cyber-crime statistics, cyber-attack.

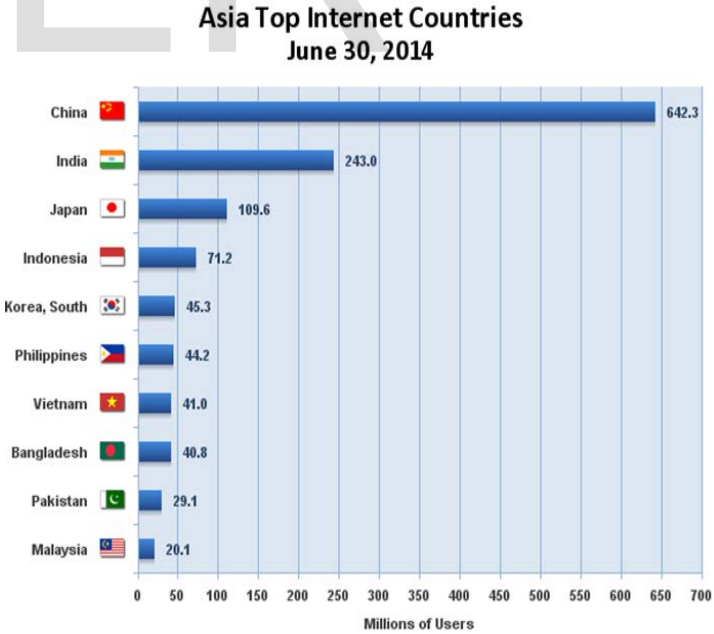
1. INTRODUCTION

These days' computer and internet become very Necessary and useful for our daily life. Today the internet is the great mediator of our lives. In present days people can get information, store information and share information through the internet. Back 20's years later there was approx.100000 people uses internet but now around 3,405,518,376 people are surf the net around the globe. The growing fastest world of internet is known as cyber world. Today cyber world are fastest moving and high technology world. Asian countries are most uses of internet in the world.



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

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.



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

2. What is Cybercrime?

Cybercrime is the latest and perhaps the most complicated problem for the cyber world. The Indian Law has not given any definition to the term 'cybercrime'. In fact, the Indian Penal Code does not use the term 'cybercrime' at any point even after its amendment by the Information Technology (amendment) Act 2008, the Indian Cyber law.

"Cyber terrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against property, government and people at large."

OR "Acts those are punishable by the Information Technology Act".

In India Information Technology Act, 2000 deals with the cybercrime problems.it covers following areas—commercial transactions online, use digital signatures defined various cybercrimes, electronic commerce.

source-
http://deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/itbill2000.pdf

2.1 Cyber Crimes Includes

Following are the few examples of cybercrime:

2.1.1 **E mail bombing:** this is a serious crime in which a person sends a numbers of emails to the inbox of the target system/person. Mail bombs will usually fill the allotted space on an e-mail server for the users e-mail and can result in crashing the e-mail server.

2.1.2 **Hacking:** among the all types of cybercrime it is the most dangerous and serous thread to the internet and e-commerce. Hacking simply refers to the breaking into the computer system and steals valuable information (data) from the system without any permission. Hacking is done by hackers now the question arises who are hackers; hackers are in b/*w* client & server and able to spoof the data/info. Duplication the IP address illegally.

2.1.3 **Spreading computer virus:** It is a set of instruction which is able to perform some malicious operations. Viruses stop the normal function of the system programs and also to the whole computer system. They can also ruin/mess up your system and render it unusable without reinstallation of the operating system A computer viruses can be spread through—Emails,Cds,Pendrives (secondary storage),Multimedia, Internet.

2.1.4 **Phishing:** phishing simply refers to steal information like passwords, credit card details, usernames etc. over the internet. Phishing is typically carried out by email spoofing and instant messaging. In this type of crime hackers make a direct link which directs to the fake page /website which looks and feel like identical to the legitimate one.

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

Source-
https://cybercrimelawyer.wordpress.com/category/66c-punishment-for-identity-theft/

2.1.6 **Internet fraud:** Internet fraud can occur in chat rooms, email, message boards or on websites. In internet fraud criminal can send fake info to the victim in cases like online purchasing, real estate, pay BAL, Work-at-home donation processing etc.

2.1.7 **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.

2.1.8 **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.

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

2.1.10 **SMS Spoofing:** SMS Spoofing allows changing the name or number text messages appear to come from.

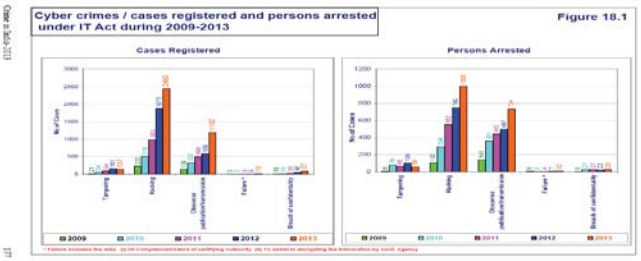
2.1.11 Voice Phishing: The term is a combination of "voice" and phishing. Voice phishing is use to gain access of private, personal and financial information from the public. Voice phishing uses a landline telephone call to get information.

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

3 Present trends of Cybercrime in India

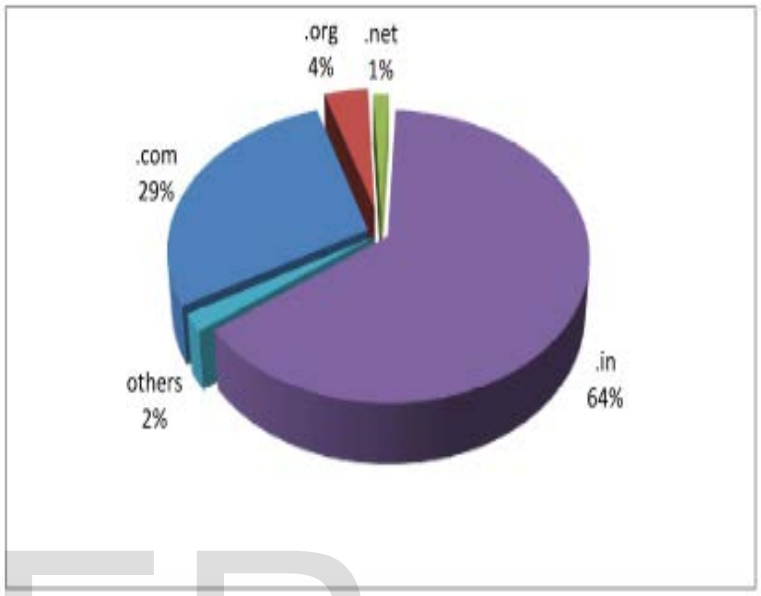
India is trying to implement the Digital India project to the best of its capabilities. The success of Digital India project would depend upon maximum connectivity with minimum cyber security risks. This is also a problem for India as India has a poor track record of cyber security.
According to Home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

In 2013, a total of 28,481 Indian websites were hacked by various hacker groups spread across the globe. The numbers of hacking incidents were 27,605 in 2012 and 21,699 in 2011.
As per the cyber-crime data maintained by National Cyber Records Bureau, a total of 1,791, 2,876 and 4,356 cases were registered under the Information Technology Act in 2011, 2012 and 2013, respectively. A total of 422, 601 and 1,337 cases were registered under cyber-crime related sections of the Indian Penal Code in 2011, 2012 and 2013, respectively.
There has been an annual increase of more than 40 per cent in cyber-crime cases registered in the country during the past two-three years,



Source-(http://ncrb.nic.in/)

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.



Source-*http://www.cert-in.org.in/*

4 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.

Source-
http://police.pondicherry.gov.in/Information%20Technology%20Act%202000%20%202008%20%28amendment%29.pdf

5 Penalty 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.

6 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.

7 Best Practices for Prevention of Cybercrime

Below mentioned security guidelines and good practices may be followed to minimize the security risk of cybercrime:

7 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

7.1 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.

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

7.3 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.

7.4 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 types 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.

7.5 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:

7.6 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.

7.7 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 a fraudulent, malicious Web sites.

7.8 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.

7.9 Guard your email address. Spammers and phishers 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.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 smileys, 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.

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

8 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.

9 Future work

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.

10 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] Introduction to Indian Cyber Law (2008) by Rohas Nagpal, Asian School of Cyber Laws, Pune, India
[4] Cyber Crime (2003) by R.K. Suri and T.N. Chhabra, Pentagon Press, New Delhi, India.
[5] http://en.wikipedia.org/wiki/Computer_crime
[6]https://cybercrimelawyer.wordpress.com/category/66c-punishment-for-identity-theft/
[7] http://ncrb.nic.in/
[8] www.economictimes.indiatimes.com/
[9] http://in.norton.com/
[10] www.ncpc.org
[11]http://www.enotes.com/research-starters/social-impacts-cyber-crime
[12]https://cybercrimelawyer.wordpress.com/category/66c-punishment-for-identity-theft/