Cyber Crime and its Related Aspects under I.T. Act, 2000 and its Prevention

Priya Singh
M. Tech. scholar
CSE Dept. MIET,
Meerut, India

Neeraj Saini
M. Tech. scholar
CSE Dept. K.E.C.,
Ghaziabad, India

Rajkumar Saini
M. Tech.,
CSE Dept. KNIT,
Sultanpur, India

ABSTRACT
Cyber Crimes are increasing day by day and are posing a great threat to internet users. This paper discusses the Cyber crime, its nature and types. Various tools and techniques used for cyber crime are evaluated in this paper. The paper also discusses cyber related laws under Indian Penal Code and their application to the cyber offences. With the discussion of cyber crimes, this paper proposes the strategies to prevent cyber crimes and recommend policies for cyber crime prevention.

Keywords
Cybercrime, Password, Indian Penal Code, Internet, E-mail, Cyber security

1. INTRODUCTION
In the current cyber world, Cyber crime is perhaps the most recent and troublesome issues. "Any criminal or illegal activity done with the help of a computer is a Cyber crime. This illegal instrumental activity could be either done to harm the target host at that time or as means to perpetuate further crimes". [1]

In simple words, Cyber crime can be understood as an "unlawful acts wherein the computer is either a tool or a target or both". It would be unsuitable to define cyber crimes as the acts punishable under Information Technology Act. Many other cyber crimes like cyber defamation, e-mail spoofing are also covered under Indian Penal Code. [1]

2. FEATURES OF CYBERCRIME
The challenges which are posed by these crimes or conducted via online environment may seem less severe through their nature; however, the way in which they are conferred is critical and most affecting. These Cyber criminals can work from anyplace on the planet, focusing on substantial quantities of individuals or organizations crosswise over universal limits, and there are great challenges which they pose through the scale and volume of the crimes they can perform by sitting on a single place in the world. It also becomes difficult to identify from which part of the world the crime is done. This increases the difficulties to recognize the culprits and bring them under the law for justice. As it is a belief that the law struggles to find these criminals and operate through the online world, the web opens many new chances to these cyber criminals enabling them to seek inside this cyber crime world. [2]

From the perspective of the child protection a key issue appears on internet which is the circulation of child sexual abuse material in huge volumes. However, this is not the major problem, the problem is the ease with which this content is circulated and offers young sexual stalkers chance to connect with others and exchange or disseminate content, and in addition, the chance to get to new casualties, either online or through offline spaces. For example, texting or long range interpersonal communication on social networking sites. Online paedophile systems can undoubtedly keep running into a huge number of suspects around the world. [2]

While the offense carried out may be conspicuous, digital crimes represent various noteworthy troubles for conventional policing over a wide range of crimes conferred on the web. While not many of them apply to this situation, they are unmistakably recognized as issues in a large portion of the examinations carried by law enforcement. [2]

3. TECHNICAL COMPLEXITY
Often cyber crime involves technically complex investigations by its nature. It requires special access to private data with specialist skills and support from various sectors. It is difficult and time consuming process to gather evidences for the crimes held online, especially when the data of evidence used in crime is routed through different countries. [2] For example, to track those who are running paedophile peer-to-peer file sharing networks or to find the ones behind fraudulent websites, law enforcement requires significant efforts.

4. LACK OF GOOD SECURITY PRACTICE
The general population and business class understands the need to have legitimate security set up, due to the emergence of numerous types of crimes. There are various anti-crime methods that the business world and common people use as measures to protect their properties like securities on cars or house locks. The same methodology is obliged on the web, yet the multifaceted nature of the specialized answers for giving security online can be befuddling and hard to comprehend for a few clients. Also, there are many data breaches which are not linked to technology, however, are caused due to carelessness or poor practices. [2]

Many people use internet with comfort from their office or home as this is the nature to access internet. However, their relaxing minds make them unaware of the threats that would not be the situation if a man was disconnected from the net.

5. TYPES OF CYBERCRIME
The activities carried out with criminal intentions in the cyber world come under Cyber crime and are broadly divided in three categories: [3]

5.1 Those against Persons [3]

5.1.1 Gambling over Internet

About of thousands of websites offers gambling over the internet and many of them are believed to be running for money laundering.

5.1.2 E-Mail Spoofing

A spoofed E-Mail is a forged electronic mail as it appears to be sent from a genuine source; however, its source is not the same which the receiver thought to be.

5.1.3 Financial Claims

The Financial Claims comprise the cases of money laundering, credit card frauds, online cheating and other such activities.

5.1.4 Selling Unlawful Articles

The sale of illegal articles includes sales of narcotics and wildlife, weapons, etc., over internet through bulletin boards, websites or using E-Mails.

5.1.5 Forgery

By the use of advanced and sophisticated computer software and hardware like scanners or printers, fake mark sheets, forged currency notes, revenue and postage stamps, etc., can be easily developed.

5.1.6 Unauthorized Publishing of Cyber Pornography

This includes pornographic e-magazines or pornographic websites created over internet through computers comprising of downloading, uploading and transmission of pornographic photos, movies, writings, video clips, etc.

5.1.7 Cyber Defamation

This may include publishing of defamatory or offensive matter over the internet about someone or sending defamatory E-mails to someone or his friends.

5.1.8 Crimes Relating Intellectual Property

This category includes trademark violations, copyright infringement, pirating software, etc.

5.2 Those against Commercial and Non-Commercial Firms and Organizations [3]

5.2.1 E-Mail Flooding

E-mail flooding also known as E-mail Bomb, is an online activity of sending huge number of E-mails to the victim's e-mail address resulting in the overflow of the mailbox of the victim.

5.2.2 Denial of Service

Denial of Service is flooding the computer server or resources with thousands of requests at a time which leads to the performance degradation of the computer server. The computer server may thus, perform very slowly or may even deny giving services. Thus, the legitimate users are also unable to use the services offered by the server. This may sometimes be done to test the performance of the server.

5.2.3 Trojan horse

A Trojan is a harmful code that seems to be an authorized program but harming the system, thereby concealing what it is actually doing. E.g. a virus pretending it to be an image but actually have malicious code scripted behind it, as user opens the image it comes in action.

5.2.4 *Data Diddling*

The concept of data diddling includes alteration of raw data immediately before processing it and then later after the completion of processing the data changing it back.

5.2.5 Salami Attack

These include the attack assigned for financial crimes. In this attack a very insignificant modification is done the important financial data which remains completely unnoticed. For e.g., running a code in the financial server of a bank which may deduct a very minute amount from the account of every customer which remains unnoticed by the customer.

5.2.6 Worm/Virus

These are software programs which fix themselves to files on computer and then move and create copies of them by attaching with other files on other computers over the internet. They affect the computer data by altering or deleting information. The difference between the worms and viruses is that worms do not require any host to attach and create their copies.

5.2.7 Illegal Access to the Computer System or Network

Getting an unlawful access to someone's personal data is called hacking. Under Indian Law, the term hacking is given a different connotation.

5.2.8 *Logic Bomb*

These programs perform their tasks on a certain event/logic as they are designed to trigger on a special occasion. For e.g., some virus may flow over the internet to attack on the New Year's Eve.

5.2.9 *Looting of some information or data enclosed in electronic form*

The data stored in the hard disk drives, CDs, DVDs, Pen Drives, or other removable storage media, etc. connected with the internet network can be looted or enclosed.

5.3 Crime Targeting the Government

Cyber crimes not just challenge the integrity of the general public, but they pose large number of threats to the Government as well. Criminals may use the internet to attack the government services for the general public with an aim to have a financial gain or to gather information about the individuals. [3] The increasing online services of the government for the public welfare provide such criminals opportunities to perform their malicious deeds.

Deceitful applications for various services, for example, benefits or tax credits, and repayment of tax may be seen by offenders to be less observed and monitored or to offer more secrecy and less human connection than more conventional extortion would require. This creates risk to increasing procurement of services over internet by the Government and will prompt more endeavors to dupe Government. [3]

6. TOOLS AND TECHNIQUES USED IN CYBERCRIME

6.1 Port Scanner

A technique used to identify the active port or the port in use over the network by the hackers or crackers is Port Scanning. Through the use of various hacking tools, a hacker can send data over the ports at a time to UDP or TCP. A response is generated from these ports which the hacker receives and can determine whether the port is in use or not. With the received

response the hacker can also focus on their attack on ports which are open and then try to gain access by exploiting any weaknesses. [3]

6.2 Password Cracking

During the login session, all systems cache passwords in the memory. Thus, the hacker may try to gain access to the memory of the system in order to sift the memory so that the stored passwords can be accessed. This task can be performed frequently by the hacker by sifting files for passwords. Cracking a password implies decrypting it or bypassing its protection scheme. Another method of cracking a password include combining letters, symbols or numbers to form the all possible combinations of a password and then trying them one by one to find the correct password. [3]

6.3 Packet Sniffing

Capturing the data packets flowing across the computer network is packet sniffing. A particular device or software used to perform this task is a packet sniffer. It can also be done to monitor the performance of the network or to troubleshoot any problem in the network. Packet Sniffer can monitor the data of the students or teachers in an educational institute to stop them from any unauthorized activity over internet. [3]

6.4 Key Logger

A key logger is a device or software which can monitor the key presses on the keyboard of a computer system and record them and thus, by installing this device or software, all the keys typed by the user can be viewed. Thus, by getting access to all the keys typed by the user, any hacker can get the information or the user passwords typed by the user which he doesn't wish others to know. [3]

7. THE COGNIZABLE AND NON-COGNIZABLE OFFENCES

Offences in which arrest without warrant is provided are called "cognizable offences" and others are "non-cognizable offences". According to the First Schedule of the Code Criminal Procedure or under any other law in force, if a police officer may arrest without a warrant, it is a cognizable case. Cognizable offence comes under cognizable case. However, a non-cognizable offence comes under a non-cognizable case, in which a police officer cannot arrest anybody without a warrant. [4]

8. SECTION 80 IN THE INFORMATION TECHNOLOGY ACT, 2000

This section defines the authority of a police officer or any other officer to enter, search, etc. [4]

(1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), under this Act, no police officer below the rank of the Deputy Superintendent of Police, or any other officer authorized by the Central Government in this regard of either the State Government or the Central Government, is allowed to enter into a public place for search or arrest any person who is suspected of being about to commit or having committed any offence without a warrant.

Intended for the reasons of this sub-section, the phrase "public-place" incorporates any public transportation, any shop, any hotel or some other spot expected for the utilization by or available to people in general.

(2) Where any individual is captured under sub-section (1) by an officer other than a cop, such officer might, immediately, take or send the individual captured before a magistrate having charge for the situation or before the officer accountable to a police headquarters.

(3) The Code's procurements of Criminal Procedure, 1973 should, subject to the procurements of this area, applied, so far as may be, in connection to any passage, inquiry or capture, made under this section.

It needs to be reiterated that section 80 applies only to offences defined and made punishable under the IT Act, 2000. It has no applicability to cyber crimes under other laws. For instance, defamation through e-mail is no offence under the IT Act, 2000. Section 80 would not apply to such case. The said offence is covered under Chapter XXI of Indian Penal Code, 1860 and would be governed by the requirements of the Criminal Procedure Code, 1973.

The elements of sub-section (1) of section 80 are the following:

- The authority to enter any public-place and pursuit and capture without warrant any individual discovered in that, is vested just in a cop not beneath the rank of a Deputy Superintendent of police (called "DSP" in short) or some other officer of the Central Government or a State Government who is approved by the focal Government;
- This force can be practiced just in "public-place" which according to the Explanation to section 80 incorporates any open transport, any lodging, any shop or whatever other spot planned for utilization by, or available to general society;
- This authority to enter any public-place and inquiry and capture without warrant any individual discovered in that, can be practiced just on the ground that such individual is sensibly associated with having conferred or of submitting or of speaking the truth to submit any offense under the IT Act, 2000.

India has sanctioned the first I.T. Act, 2000 taking into account the UNCIRAL model prescribed by the general gathering of the United Nations. Section XI of this Act manages offenses/law violations alongside certain different procurements scattered in this Acts .The different offenses which are given under this part are demonstrated in the accompanying table:

Table 1. Offence And Related Section Under I.T. ACT [5]

Offence	**Section under IT Act**
Publishing False Digital Signature Certificates	Section 73
Privacy and Confidentiality Breach	Section 72
Accessing Unauthorized Protected System	Section 70
Publishing Obscene Information	Section 67

Data alteration and Hacking Computer System	Section 66
Tampering documents sources with Computer	Section 65

NOTE: Section 78 of I.T. Act empowers Deputy Superintendent of Police to investigate cases falling under this Act.

Table 2. COMPUTER RELATED CRIMES COVERED UNDER IPC AND SPECIAL LAWS [5]

Offence	**Section**
Sales of Arms Online	Arms Act
Sales of Drugs Online	NDPS Act
E-mail Abuse	Section 500 of IPC
Web Jacking	Section 420 of IPC
E-mail Spoofing	Section 463 of IPC
Cyber frauds and Bogus websites	Section 383 of IPC
Forging electronic records and data	Section 463 of IPC
Sending defamatory e-mail messages	Section 499 of IPC
Sending threatening e-mail messages	Section 503 of IPC

9. STRATEGIES TO PREVENT CYBERCRIME [6]

Cyber criminals are similar to conventional or traditional criminals in the way that they need to profit as fast and effortlessly as would be prudent. Cybercrime can be prevented in a cost-effective and quick manner. Cybercrimes can be avoided by common sense and also if some technical advice is taken similarly as hardening the target for a business or residence through alarms, locks or lights. If the cyber criminal finds the target difficult to attack, he is more likely to leave it and move to an easier target. The accompanying ten tips are fundamental ways in which the cybercrime can be avoided.

9.1 Choose a secure/ strong password and keep it safe

Usernames, passwords, and individual distinguishing proof numbers (PIN) are utilized for each online exchange today. A strong secret password ought to be no less than eight characters long with a blend of letters and numbers. Utilizing the same secret password for different websites or systems expands the danger of disclosure and conceivable abuse. It is never a decent practice to record a secret password and keep it close to the system it is expected to be utilized on. Changing a secret password at regular intervals is a decent practice to confine the measure of time it can be utilized to get to sensitive data.

9.2 Keeping the System up to date

Cyber offenders will utilize flaws in software to assault PC frameworks anonymously and repeatedly. Most Windows based frameworks can be arranged to download programming fixes and upgrades consequently. This will avoid and impede the cyber criminals who exploit software package flaws. This will likewise hinder various computerized and basic assaults offenders utilize to break into your framework.

9.3 Secure System Configuration

It is essential that PCs are designed to the security level that is proper and agreeable for the client. An excess of security can have the antagonistic impact of disappointing the client and perhaps keeping them from getting to certain web content. Utilizing the "help" highlight of the working system can frequently address a number of questions around this area.

9.4 Install and regularly update antivirus software

It is a software program designed to remove and avoid the malicious codes or software programs embedded into the computer system. On detection of a malicious code, it works to remove and disarm them. These malicious codes could be virus or worm. Virus infect the system without the knowledge of the user, thus, antivirus software is designed to update automatically on its own. About 100 percent of the PCs sold in the United States today accompany some type of antivirus programming. Inability to keep this product updated is a great emerging issue. The firewall screens all information streaming all through the system to the Internet, regularly, and blocking assaults coming in and out of the system. Antivirus programs are the next barrier to Cyber Crimes observing all online action with the goal to shield the computer from infections, different malicious codes, and can upgraded to more security by securing against spyware and adware. To be protected on the Internet, the antivirus programs ought to be arranged to upgrade it each time the computer interfaces with the Internet.

9.5 Turning on the Firewall

Firewall protects the system and the internal network from the hackers in the outer network trying to gain access to the system and crash it, steel password and other sensitive data or delete information. Firewall software already comes with some operating systems or it may also be purchased for personal use. In case of multiple networks, firewall protection is provided by the hardware routers.

9.6 Protecting one's Personal Data

Using a considerable amount of the online facilities today includes sharing fundamental individual data incorporating name, personal residence, telephone number, and email address. Utilizing judgment skills is the most ideal approach to ensure protection against cybercrime. Try not to react to email messages that contain incorrect spellings, poor language structure, odd expressions, or sites with unusual expansions, if there is doubt about reacting to an email. Consider a phone call to the association to check genuineness. Instead of clicking the link for a website, consider typing the address on the web browser. Check that the URL contains an "s" after "http", i.e., "https" before going for any financial transaction on the website. This "s" stands for secure and it must appear in the URL requesting you to enter your login details or while providing other sensitive data. Another secure connection sign is a small lock icon which appears in the bottom of web browser usually to the right.

9.7 Read the fine print on site security strategies

On numerous photograph sharing and social networking websites, there is wording on the protection policies that permit the site to record data and photographs as often as possible which are posted to those sites, even after the post has been erased by the client. While this may not demoralize one from posting pictures or messages, mindfulness that this can be later recovered and spread may be a thought in the matter of what data or photographs are posted. What today may appear to be a safe trick can have a shocking impact on one's reputation quite a long year later when applying for an occupation or other opportunity?

9.8 Avoid Scamming

Think several times before clicking any link or a file which as no authentic origin. It would be wise to avoid such e-mails and check the message source. Always verify the source when in doubt and never reply to any e-mails asking for your personal and financial information or user ID and password.

9.9 Review money related statements routinely

Reviewing credit card and bank statements frequently will regularly diminish the effect of wholesale fraud and credit misrepresentation by finding the issue not long after the information has been stolen or when the first utilization of the data is endeavored. MasterCard insurance services can regularly alert a man when there is strange activity happening on his or her record. For instance, purchasing in a geologically far off area or a high volume of purchasing should be taken as endangered activity. These alarms ought not to be taken carelessly and could be the first indicator that a person gets about something isn't right.

9.10 If it appears to be unrealistic, it is

No one is going to get a huge whole of cash from a dead Nigerian government official, win a colossal lottery from being "haphazardly chosen from a database of email addresses," or profit from "aloof remaining wage a couple of hours every day working out of your home." Many of these unlawful acts go unreported on the grounds that the casualty is excessively humiliated, making it impossible to admit to law requirement that they were tricked.

9.11 Turn your computer off

Many people opt for leaving their computers on and ready to use due to the growth of high speed internet connections. However, the downside of this is always being neglected. Beyond the protection of firewall, designed to obstruct unwanted attacks, it is also a good practice to turn the computer off when not in use as it disconnects it from the network and avoids the attacker's connection or a spyware used to employ the resources of your computer. The major learning is that every step taken to avoid these threats, keeps you away from becoming a cybercrime victim.

10. POLICIES RECOMMENDED FOR CYBERCRIME PREVENTION [6]

By implementing the following policies and practicing them regularly, the cybercrimes can be avoided:

1. The lack of trained human resource and finances pose a basic issue in developing cyber society. To ensure the effective benefits from information system, integrated policies are required.
2. To secure the society from cyber crimes, the society should follow a strong education system, delivering education at every stage of society stressing especially on Information Technology which will make the common man more alert towards these crimes.
3. The core part of Information and Communication Technologies (ICTs) should be promoted in Research & Development area and also in Resource Development of the system.
4. To foster highly secure and quality services and production adopt the standards of ICTs' quality assurance and regulation to keep competition and benefit the communities within countries.
5. To create an information society which is free from cyber crime, common, up to date and mutually supporting cyber laws should be set up against the cyber crimes and protecting the rights of intellectual property.
6. High levels of mindfulness among the every section of the general public ought to arrive with respect to data security and digital crimes and expanded trade of data on data security and digital crime at the territorial and national levels must be set up.
7. Conduct national awareness campaigns for the general client, including kids and youngsters, educational foundations, purchasers, government authorities and the private sector, utilizing distinctive media.
8. Effective systems must be set to recognize and prevent digital offences and enhance security against, identification of, and reactions to, digital offences, at the lower level itself.
9. Educate and include the media experts, and after that urge them to expand pubic alertness.
10. Engage expansive private segment corporations and industry relationship in the sponsorship of mindfulness projects.
11. Stress ought to be laid on less developed nations on successful frameworks, for protecting against, recognition of and responses to, digital offences.
12. Measure the concern of safe environment over internet for children and promote and support software which uses filtering, parental control, ratings, etc.
13. Law requirement staff must be educated and prepared to address high-tech crimes.
14. Legal systems ought to allow the safeguarding of and brisk access to electronic information, which are regularly discriminating to the fruitful examination of offences.
15. Mutual help regimes must ensure the convenient assembling and interchange of proof in cases including international high-tech offences.
16. Use the built up system of educated work force to guarantee a timely, viable reaction to transnational cutting edge cases and assign a state of-contact who are available on a 24-hour premise.
17. Prevention is superior to any cure. Increasing awareness, instruction, and specialized support to avoid e-crimes is necessary, but without disheartening the advancement of e-trade.

11. RECENT SCENARIO OF CYBERCRIME: CHART FOR TOP-20 COUNTRIES

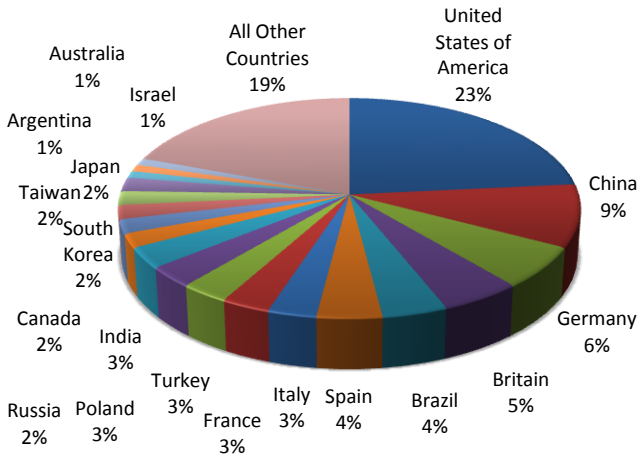

Fig 1: Cybercrime: Top 20 Countries [7]

12. CONCLUSION

Cybercrime is now became the problem of every individual. It has threatened the whole society and the nations. Not only students, professionals, organizations, it has affected the government and the nations throughout the globe. There is no doubt that the Internet offers crooks unparalleled open doors. Information and the cyber awareness is the best type of security. Every individual must be brought to awareness about the cyber crimes so that one can take protective action by educating them the Do's and Don'ts over the internet. Powerful measures must be found with a specific end goal to track evidences in electronic media, group the material that needs search, and their conservation, so that the systems are better shielded from digital interruptions. Moreover, new principles and regulations must be created by law authorization offices to address the cyber offences.

13. REFERENCES

[1] P.A. Singh, A. Bhardwaj, and S.G. Dangayach. "Ethical values and practices for cyber society." *In Current Trends in Information Technology (CTIT), 2009 International Conference on the*, pp. 1-5. IEEE, 2009.

[2] "Cyber Crime Strategy." Internet: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf [August 28, 2015]

[3] V.S. Kumar. "Cyber Crime- Prevention & Detection." Internet: http://www.indiancybersecurity.com/downloads/cci/Cyber%20Crime%20Investigation%20.pdf [August 26, 2015].

[4] S. Vivek, Cyber Law Simplified. Tata McGraw-Hill Education, 2001, p.11.

[5] S. Vivek, Cyber Law Simplified. Tata McGraw-Hill Education, 2001, p.5.

[6] National Crime Prevention Council. "Cybercrimes." Internet: http://www.ncpc.org/resources/files/pdf/internet-safety/13020-Cybercrimes-revSPR.pdf [September 2, 2015].

[7] "Top 20 Countries Found to Have the Most Cybercrime." Internet: http://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/ [August 28, 2015].