EMERGING TRENDS IN INDIAN CYBER CRIMES

by Dr. Upendra Nath Tiwari

Assistant Professor, Shri Ramswaroop Memorial University, Uttar Pradesh

INTRODUCTION

The invention of Computer has made the life of humans easier, it has been using for various purposes starting from the individual to large organizations across the globe. In simple term we can define computer as the machine that can stores and manipulate/process information or instruction that are instructed by the user. Most computer users are utilizing the computer for the erroneous purposes either for their personal benefits or for other's benefit since decades[1]

This gave birth to "Cyber Crime". This had led to the engagement in activities which are illegal to the society. We can define Cyber Crime as the crimes committed using computers or computer network and are usually take place over the cyber space especially the Internet.

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 The government in India promotes the adoption of IT based products and IT enabled services in public services such as citizen services, citizen identification, public distribution systems etc. The availability of computerized bank operations have brought millions of people exposed to the cyber world.[2]

As a result of commoditization of technology the accessibility and ease of use of computers have resulted in a situation where many persons are perfectly able and efficient in using their systems. The collective diminution in general computing ability level of users give rise to acknowledged gap between the expert and non expert user. The exploitation of this gap is a key driver of cybercrimes.

What is cyber space and cybercrime?

Internet is otherwise known as Cyberspace. Cyberspace is anonymous and borderless unlike physical space. In general, the nature of Internet and its relative anonymity enable individuals to behave differently from the physical world. Also, the cyberspace renders virtual environment where anybody can blot out his identity on the network and creates a false name or can take on some other identity. The risk in cyberspace is multiple. They threaten personal data security. Victims on the whole suffer financial loss through frauds and get defamed by willful perpetrators. Therefore, online risks may often lead to physical or mental harm or both to the individual[3]. Cybercriminals can effectively function from any place in the world in many disguises and intermediaries and target large number of people or businesses all around international boundaries. Therefore the challenges are wide, varying and great in magnitude.

---

1 www.tigweb.org/action tools/projects/download/4926.

2 ministry of Communication and Information Technology, India's National Cyber Security policy NSCP) 2013

3 Standing Committee on Information Technology 2013-14, Cyber Crime, Cyber Security And Right To Privacy, 52nd Report, Fifteenth Lok Sabha Secretariat, New Delhi. 2014.

Although 'cybercrime' is repeated daily by many there is no commonly accepted definition of it. Generally, it denotes any criminal offence committed with oid of or against a computer network. The cyber-crimes again are of two types: new offences committed using new technologies and old offences committed using new technology. In both situations, the networked devices are used to finish the commission of an offence. Cyber-crimes can also be in the form of organized cyber attack, theft of data from corporations and governments.[4]

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 cyber crime problems. it covers following are as commercial transactions online, use digital signatures defined various cyber crimes, electronic commerce.[5]

History of Cyber Crime:

The first Cyber Crime was recorded within the year 1820. The primeval type of computer has been in Japan, China and India since 3500 B.C , but Charles Babbage's analytical engine is considered as the time of present day computers.

In the year 1820, in France a textile manufacturer named Joseph Marie Jacquard created the loom. This device allowed a series of steps that was continual within

The weaving of special fabrics or materials. This resulted in an exceeding concern among the Jacquard's workers that their livelihoods as well as their traditional employment were being threatened, and prefer to sabotage so as to discourage Jacquard so that the new technology cannot be utilized in the future[6].

Evolution of Cyber Crime

The cyber crime is evolved from Morris Worm to the ransom ware. Many countries including India are working to stop such crimes or attacks, but these attacks are continuously changing and affecting our nation

Evolution of Cyber Crime

Years	Types of Attacks
1997	Cyber crimes and viruses initiated, that includes Morris Code worm and other.
2004	Malicious code, Torjan, Advanced worm etc.
2007	Identifying thief, Phishing etc.
2010	DNS Attack, Rise of Botnets, SQL attacks etc
2013	Social Engineering, DOS Attack, BotNets, Malicious Emails, Ransomware attack etc.
Present	Banking Malware, Keylogger, Bitcoin wallet, Phone hijacking, Anroid hack, Cyber warfare etc.

Classifications of Cyber Crime

- **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.

---

[4] http://www.phiprivacy.net/nhs-england-patient-data-uploaded-to-google-servers-tory-mp-says,/Last accessed l9 August 2014.

[5] http://deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/itbill2000.pdf

[6] https://www.ijarcsse.com/docs/papers/Volume_3/5_May2013/V3I5 0374.

- **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
- **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.
- **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.
- **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. [7]

- **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.[8]

- **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.

- **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 allows changing the name or number text messages appear to come from.

- **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.
- **Software piracy**: It can be describes as the copying of software unauthorized.
- **Copyright infringement**: It can be described as the infringements of an individual or organization's copyright. In simple term it can also be describes as the using of copyright materials unauthorizedly such as music, software, text etc.[9]

---

[7] https://cybercrimelawyer.wordpress.com/category/66c-punishment-for-identity-theft/

[8] Law and emerging technology cyber law and E-commerce 4th edition by Adv. Vakul Sharma pg 150

- **DOS attack**: In this attack, the attacker floods the servers, systems or networks with traffic in order to overwhelm the victim resources and make it infeasible or difficult for the users to use them[10]

Cyber Crime's scenario in India (A Few Case study)

a) The Bank NSP Case
In this case a management trainee of a bank got engaged to a marriage. The couple used to exchange many emails using the company's computers. After some time they had broken up their marriage and the young lady created some fake email ids such as "Indian bar associations" and sent mails to the boy's foreign clients. She used the banks computer to do this. The boy's company lost a huge number of clients and took the bank to court. The bank was held liable for the emails sent using the bank's system[11]

b) Bazee.com case
In December 2004 the Chief Executive Officer of Bazee.com was arrested because he was selling a compact disk (CD) with offensive material on the website, and even CD was also conjointly sold-out in the market of Delhi. The Delhi police and therefore the Mumbai Police got into action and later the CEO was free on bail.[12]

Parliament Attack Case

The Bureau of Police Research and Development, Hyderabad had handled this case. A laptop was recovered from the terrorist who attacked the Parliament. The laptop which was detained from the two terrorists, who were gunned down on 13th December 2001 when the Parliament was under siege, was sent to Computer Forensics Division of BPRD. The laptop contained several proofs that affirmed the two terrorist's motives, mainly the sticker of the Ministry of Home that they had created on the laptop and affixed on their ambassador car to achieve entry into Parliament House and the fake ID card that one of the two terrorists was carrying with a Government of India emblem and seal. The emblems (of the 3 lions) were carefully scanned and additionally the seal was also craftly created together with a residential address of Jammu and Kashmir. However careful detection proved that it was all forged and made on the laptop.[13]

Andhra Pradesh Tax Case

The owner of the plastics firm in Andhra Pradesh was arrested and cash of Rs. 22 was recovered from his house by the Vigilance Department. They wanted evidence from him concerning the unaccounted cash. The suspected person submitted 6,000 vouchers to prove the legitimacy of trade, however when careful scrutiny the vouchers and contents of his computers it unconcealed that every one of them were made after the raids were conducted. It had been concealed that the suspect was running 5 businesses beneath the presence of company and used fake and computerized vouchers to show sales records and save tax. So the dubious techniques of the businessman from the state were exposed when officials of the department got hold of computers utilized by the suspected person.[14]

---

[9] Cyber crimes and law by Dr. Amita Verma Central law publication edition 2012

[10] http://searchsecurity.techtarget.com/definition/denial-of-service

[11] http://www.legalserviceindia.com/lawforum/index.php?topic=2239.0

[12] Avnish Bajaj vs State (N.C.T.) Of Delhi on 21 December, 2004 (2005) 3 CompLJ 364 Del, 116 (2005) DLT 427

[13] State vs Mohd. Afzal And Ors. [Along With ... on 29 October, 2003

[14] Smc Pneumatics (India) Pvt. Ltd vs Shri Jogesh Kwatra on 12 February, 2014

SONY.SAMBANDH.COM CASE

India saw its 1st cybercrime conviction. This is the case where Sony India Private Limited filed a complaint that runs a website referred to as www.sony-sambandh.com targeting the NRIs. The website allows NRIs to send Sony products to their friends and relatives in India after they pay for it online. The company undertakes to deliver the products to the involved recipients. In May 2002, somebody logged onto the web site underneath the identity of Barbara Campa and ordered a Sony colour television set and a cordless head phone. She requested to deliver the product to Arif Azim in Noida and gave the number of her credit card for payment. The payment was accordingly cleared by the credit card agency and the transaction processed. After the related procedures of dues diligence and checking, the items were delivered to Arif Azim by the company. When the product was delivered, the company took digital pictures so as to indicate the delivery being accepted by Arif Azim. The transaction closed at that, but after one and a half months the credit card agency informed the company that this was an unauthorized transaction as the real owner had denied having made the purchase. The company had filed a complaint for online cheating at the CBI that registered a case under the Section 418, Section 419 and Section 420 of the IPC (Indian Penal Code). Arif Azim was arrested after the matter was investigated. Investigations discovered that Arif Azim, whereas acting at a call centre in Noida did gain access to the number of the credit card of an American national which he misused on the company's site. The CBI recovered the color television along with the cordless head phone. In this matter, the CBI had proof to prove their case so the accused admitted his guilt. The court had convicted Arif Azim under the Section 418, Section 419 and Section 420 of the IPC, this being the first time that a cybercrime has been convicted. The court, felt that since the defendant was a boy of 24 years and a first-time convict, a compassionate view needed to be taken. Thus, the court discharged the defendant on the probation for one year.[15]

Online frauds a headache for Delhi Cyber Cell

Cracking cases of online cheating and cyber frauds are proving to be the biggest challenge for Delhi Police despite advanced software available in the market. More than 75 per cent of cases registered with the cyber cell last year remains unsolved while criminals in the field seem to be making better use of this software to hoodwink cops.

The data compiled by Delhi Police states that out of 327 cases registered from 2017 to November 30, 2018, the probe was concluded only in 71 (21.7 per cent). Meanwhile, out of the 160-odd cases registered, the cyber cell managed to complete investigations in only 26 cases in 2018.

According to the police 'e-wallet skimming frauds' and fake customer care cyber frauds whose numbers are on the rise and are currently ruling the charts of all cybercrimes known so far.
Speaking about the modus operandi of this trending cyber fraud, a senior police officer said: "If a person is posting an advertisement of his product on OLX to sell it, the fraudsters notices it and contacts the buyer and shows interest in purchasing it. Over the phone, the unknown buyer will ask the seller to download a particular e-wallet application and accept the request which he will send from the other end."

After getting the details of QR code and reference number of the buyer, the sender sends a link which asks for approval and once it is clicked, messages of money withdrawal from the buyer's e-wallet and bank account start dropping in and the fraud gets executed, said the officer.
Most of the e-wallets are linked with credit/debit cards or bank accounts. So once the miscreants get access to the account, it is a piece of cake for him to get away with the money without the victim knowing about it, the officer added.

According to a cyber expert, it is very difficult to detect high-tech advance software that have accesses and re-routes from multi-countries, but the actual hacker has an ability to hack websites, bank accounts and e-commerce sites just by being a few metres away.

[15] http://www.cyberralegalservices.com/detail-casestudies.php

It is very difficult to access IP addresses from one country to another country and catch the accused who stays in the domestic country.

Delhi Police officers have put the blame for the delay in investigations on getting information from websites, internet service providers, social media portals and telecom firms.
However, sources said the limited technical knowhow of cyber cell members is proving to be an obstacle and resulting in slowing the investigation process.
Recently the unit busted various cybercrime modules ranging from Bitcoin cons to illegal Ethereum rigs. However, the criminals are coming up with new means to dupe people.[16]

"The criminals are one step ahead of us and are finding new software so that it becomes a task for the cyber cell to trace them. However, the unit will soon have has access to some of the latest technology, including retrieving data from a damaged hard disk or mobile phone and they in the process of acquiring more including more sophisticated software for social media analysis," the senior officer added.

Officials also stated that criminals, terrorists and antisocial elements are using social media websites and other public platforms for conversations to plot their activities. At present, Delhi Police do not have any means to extract the content available on the web and convert it into meaningful data to identify criminals or trace their conversations.

"The problem which we have been facing is that it takes time to get approvals and access to information from the tech giants such as Facebook and Twitter as the service providers don't share information easily. Recently, WhatsApp had submitted an affidavit in a city court that their encryption software is such that they can't share information leading to delay in investigation," the officer said.

The tracking of IP address has also become a task for the police, as there are websites, applications and service providers that provide VoIP numbers and they don't share information with the police, he added.

VoIP is a software which enables people to use the Internet as a transmission medium wherein the caller can use an Indian number but which will show as an international number[17].

Recently, Delhi Chief Minister Arvind Kejriwal received two threat mails on his official email. However, the police have failed to crack or get a breakthrough in that case.

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

[16] https://www.indiatoday.in/crime/story/online-frauds-a-headache-for-delhi-cyber-cell-1578578-2019-08-08

[17] https://economictimes.indiatimes.com/tech/internet/bengaluru-is-indias-cybercrime-capital/articleshow/67769776.cms?from=mdr

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. [18]

> 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.

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

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.

CONCLUSION AND SUGGESTION

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.

---

[18] Introduction to Indian Cyber Law (2008) by Rohas Nagpal, Asian School of Cyber Laws, Pune, India

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.

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

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.

References

- Cyber Crimes: Law and Practices(.pdf); retrieved from http://www.img.kerala.gov.in/docs/downloads/cyber%20crimes.pdf

- Types of Cyber Crimes & Cyber Law in India by Adv. Prashant Mali, Security Corner; retrieved from http://www.csiindia.org/c/document_library/get_file?uuid=047c826d171c-49dc-b71b4b434c5919b6

IMPORTANT WEBSITES & ADDRESSES

1. http://deity.gov.in/ Department of Electronics and Information Technology, Govt. of India
2. http://cybercellmumbai.gov.in/ Cyber crime investigation cell
3. http://ncrb.gov.in/ National Crime Records Bureau
4. http://catindia.gov.in/Default.aspx Cyber Appellate Tribunal
5. www.nic.in National Informatics Centre
6. www.idrbtca.org.in IDRBT