

Effects Of Cybercrime In India

Aaron Francis Godinho, Abhishek Jha and Krantee Jamdaade

Aaron Francis Godinho, 411, Mangalwadi, Juhu Tara Road, Santacruz(W), Mumbai

Abhishek Bipin Jha, S.N. 341, Govt. Colony, Bandra(E), Mumbai

Lecturere at L.B.H.S.S.T's I.C.A., Bandra E,
Mumbai, India

ABSTRACT

We live in the world where in each steps you find yourself surrounding with technology which is connected to Internet. As the number of internet user increases, it also opens an opportunity to the attacker to harm frequent user. There are many kind of cyber menacing by which culprit target and harm unaware people. Now the time comes when authorities have to take some solid decision and make some strict law. To make law about cybercrime we need to analyze sharply the behavior and motivation of cybercrime. This review paper includes cybercrime statistics of India and other latest news regarding cybercrime. This journal is all about the cybercrime and their impacts.

Keywords: Cybercrime, India, Effects, Crime

1. INTRODUCTION

There are many variations in both committing and prosecuting the crime between cybercrime and standard crime. Everything that seems to favor the criminals. The cybercriminal may be far from where the crime occurs most of the time. The attackers can choose where they are going to and when the crime is going to be committed because cybercrime does not require the perpetrator to have a physical presence.

The Criminal activities are done with the use of computers and the internet, specifically unauthorized trespass into the system or database, manipulating or data stored online.

One report ranked India in 2008 as the 14th country in the world hosting phishing websites. Moreover, the increase of call centers in India has increased a huge rate of cybercrimes over the data maintained online. Titled label 'Crime Online: cybercrime and Illegal Innovation', the report states that cybercrime in India, China, Russia and Brazil is because of "particular concern" and that there has been a "increase in cybercrime" in India in recent years, because of the large number of call centers[1].

Cybercrimes can be categorized as follows-

a. Data Interception

An offender monitors data which is being transferred from one place to another. This attack could be undertaken to collect the information about the victim. This attack includes sniffing traffic on the network.

b. Data Modification

Privacy of communications is important to make sure that information can't be changed or viewed in transit. Distributed environments bring with them the chance that a malicious third party will commit a computer crime by meddling with information because it moves between sites.

c. Data Theft

Data theft is normally described as data is copied or stolen illegally from a company or other person. The data stolen here is personal details like passwords, security numbers, etc. all the confidential information. This information is illegally collected, when the person who stoles the data is caught, he is prosecuted with the full extent of cyber laws.

d. IP address spoofing

It is also known as IP address stealing where the Internet Protocol (IP) address of a user is compromised using which the intruder is able to perform his activities. The legitimate user is targeted by the hijacker whose IP address is used to alter the packet headers so it appears to be the original source.

e. Email spoofing

Hacking of email ID. Hacker uses the email id of a user for the mischievous activity, this is known as email spoofing.

f. Computer virus

A computer program loaded in a user's computer and runs against his wish having the capability to damage the files and replicate.

g. Computer worm

These are the computer program which replicates itself and spreads into the targeted computers. It uses network as a medium to spread itself in the targeted computer. It is different from a virus as it doesn't need itself to be attached to an existing program.

h. Phishing

Hacker tries to steal personal information. E.g. a user gets a mail to share his account details and send sum of 3000INR to process the lottery he has won in UK.

i. Spyware

It is harmful software installed on a person's pc without his knowledge in order to steal data associated with the user.

2. IMPACTS OF CYBER CRIME

Criminals are using the internet to carry out their fraud and theft activities. Internet based crimes are increasing more and more on daily basis.

Online stock fraud has made investors lose millions per year thus leading to lose their trust in stock market. Law officials across India have said that they have seen an increase in number of crimes in recent years. As the daily man is getting more and more dependent on the internet, the information stored about him can be easily stolen.

As per the survey conducted in past, 80% of companies have accepted that they have suffered losses due to cybercrimes[2]. As the world increases its dependency on internet, the risk of being attacked will keep on increasing.

As payments are done online through credit cards more protection will be necessary. Productive time is also at risk.

Worms, viruses deployed by the attackers can make the system slow or even the servers slow making the data inaccessible. The considerable portion of e-commerce revenue is lost due to the fear of theft in the shoppers mind, creating trust issues and making business stuck.

3. IMPACTS ON BUSINESS

Now a day, cybercrime against business is growing with full speed. The reported total loss of \$265 million, \$378 million, and \$450 million was calculated in 2000, 2001, and 2002 respectively. Additionally, It is estimated that since the internet came to action among general people the total lost from 1997 to 2002 is \$2 billion, as per reported to the authorities. The very way that business is now conducted, most of the people preferred use of internet for making payment puts the business in risk of cybercrime. The increasing role of the Internet in Business sales, the huge amount of data gets transferred through the computer systems inside organizations, which are very sensitive and is related to the core of business; the immense use of Internet in the workplace; and increased access to confidential information, all of these are factors that contribute to the growing threat of cybercrime.

4. METHODOLOGY

The formal meaning of research is scientific investigation or enquiry to extract truth or discover new ideas.

Scientific research has a big role in today's era. A proper systematic application of scientific method gives proper solution to different problems. The methodology used here is secondary survey. Secondary research is done on materials already published in research. These documents are available on websites, libraries, data obtained from already filled survey. There are many resources where data can be collected and used.

This is a cost effective method, as data is easily available and isn't time consuming. The data collected in this method gives organizations an idea about what is found in the research, thus they can form hypothesis and evaluate the cost of the research. Quantitative research is depending on the quantity or amount. It is applicable to situations that can be shown in terms of quantity.

5. DATA COLLECTION AND ANALYSIS

Cybercrime victims are organizations which are affected by some external sources without their knowledge. In case of data theft, data can be stolen from the database of the organization which could include security number, credit card information, email addresses. This substantial loss of data would result in loss of customers. People can also suffer huge losses when their confidential information is stolen. Now we all know that, India already is the second-largest online market worldwide.

Among Indian states, Maharashtra topped the list in 2018. Other vital business hubs with good developing rate such as Delhi and Telangana were also among the 12 most affected regions.

Indian states most affected by Cyber attacks

1. Maharashtra
2. Delhi
3. West Bengal
4. Gujrat
5. Uttar Pradesh
6. Karnataka
7. Rajasthan
8. Tamil Nadu
9. Madhya Pradesh
10. Telangana
11. Hryana
12. Odisha

Not only the metro city but non metro cities like Jabalpur, Patna, Bhubaneswar are take place in top 15 city of India which is most affected by cyber threat according to recent report by Quick Heal.

Cities with most risk of Cybercrime attacks are

1. Mumbai
2. Delhi
3. Bengaluru
4. Kolkata
5. Pune
6. New Delhi
7. Hyderabad
8. Jaipur
9. Ahmedabad
10. Chennai
11. Jalalpur
12. Bhubaneswar
13. Thane
14. Gurugram
15. Patna

6. SCENARIO OF CYBER CRIME IN MUMBAI

Crime Detection in Mumbai

Every day about 3 to 4 cases of cybercrime are being filed in the city on an average, but detection rates remain low. In the last two years, 2,723 cyber offences were filed and the police managed to solve only 362 (13%). This detection rates have jumped from only 8% in 2017 to 19% in 2018.

Table 6.1: Crime Detection in Mumbai

Year	2018	2017
Crime Reported	1362	1361
Crime Detected	260	102

Crime Solving Rate in Mumbai

Mumbai is the financial capital of India. Large number of people here does their transaction of money through Internet. Daily new people are joining that club. The numbers also increases the chances of risk. In city like Mumbai where population is more than million, hardly 1000 of police are well trained for solving the cyber related cases.

When we look deep down in it we found that, the total cybercrimes solved in 2019 decreased to 15.1% (498 cases and 75 solved till April end) against 67.7% detection (62 cases and 42 solved) in 2012.

Table 6.2: Card Fraud cases in Mumbai

Year	2019	2018	2017	2016	2015	2014	2013
Cases Filed	153	461	606	423	320	183	32
Solved	8	28	24	54	36	22	20
Percentage	5.2	6.1	4	12.8	11.3	12	62.5

7. FUTURE ENHANCEMENT

Below mentioned are some guidelines and good practices to keep a check on cyber-crimes.

By updating your computer: To avoid cyber- attacks, always update your computer’s operating system with antiviruses regularly. Keeping the antivirus up to date will make it difficult for the hackers to access the system and block any automated attacks.

By setting strong password: Always set a password which has minimum of characters, which are combinations of letters, numbers and symbols (e.g. # \$ % ! ?). Do not keep simple passwords like name, city and try to use non dictionary words. Store password in safe place and don not use similar password for every service online. Change passwords regularly.

By installing a security software: This includes firewall and anti-virus programs. Firewalls are first line of defense of the computers. Anti-virus scans all the online activities carried out and protect computers from worms, viruses, Trojan horses and other harm full programs. Security updates should be configured to update itself every time it connects to the computer.

By shielding personal information: Never respond to email messages that ask for personal information, companies never use email to ask for personal information. Always try typing URLs directly in the web browser then clicking on URLs present in the email messages.

Keep a check on bank details regularly: Regularly check on the bank details and other card details belonging to you. Now days many banks are installing fraud prevention systems that detects fraud if taking place in form of unusual purchasing behavior.

Mobile devices: Always be aware of viruses and hackers trying to get inside your mobile devices. Download apps and games only from official sources. **Secure your social media:** Never post any type of personal information on social media.

Secure your WiFi: Setup proper home network and always keep changing your password. Avoid using public WiFi hotspots.

Call the right person: If you are victim by any type of cybercrime, always call the local police. If any maintenance or software update required, always consult the authorized authenticated personnel or a certified computer technicians.

8. CONCLUSION

This report is focused on making known the effects of cybercrimes and also explains the impacts on the society. In this new era of modern world criminals have changed their method and started using advanced technology. All kind of cybercrime is happened due to lack of awareness. This is a duty of Government, media houses to educate all the internet users about the risks of the cyber-world, prevention is always better than cure.

Government should teach the common man about the risks of cyber-world, this will show the community how to protect all the critical information which is present online. Yet India has to take a lot of steps to stop cybercrime, the cyber law has to keep changing with time. Thus upgrading laws as technology upgrades.

REFERENCES

- [1] H Saini, YS Rao, TC Panda, "Cyber-crimes and their impacts: A review" International Journal of Engineering ..., 2012 - academia.edu
- [2] "Mumbai: Only 21% of cyber crime cases solved since 2012" https://timesofindia.indiatimes.com/city/mumbai/mumbai-only-21-of-cyber-crime-cases-solved-since-2012/articleshow/69708717.cms?UTM_Source=Google_Newsstand&UTM_Campaign=RSS_Feed&UTM_Medium=Referral
- [3] "High alert: Not just big cities, even small town India is prone to cyber attacks" <https://scroll.in/article/923846/high-alert-not-just-big-cities-even-small-town-india-is-prone-to-cyber-attacks>
- [4] Nick Nykodym, Robert Taylor, Julia Vilela, "Criminal Profiling and insider Cyber Crime" Elsevier
- [5] Vinit Kumar Gunjan, Amit Kumar Sharda Avdhanam, "A survey of Cyber Crime in India"
- [6] Quick Heal Annual Threat Report 2019
- [7] Brayn Watkins "The Impacts of Cyber Attacks on Private Sector August 2014"

AUTHOR



Abhishek Jha has done BCA from Magadh University Bodhgaya in 2016 and right now pursuing MCA from L.B.H.S.S. T's I.C.A. Bandra E from Mumbai University.



Aaron Francis Godinho has done B.Sc IT from Mumbai University Mumbai in 2016 and right now pursuing MCA from L.B.H.S.S. T's I.C.A. Bandra E from Mumbai University.



Krantee Jamdaade has done MCA from Mumbai University in 2006 and received M. Phil. (CS) degree from YCMOU Nashik in 2011. Now pursuing Ph. D. (CS) from Mumbai University under the guidance of Dr. Seema U. Purohit and working as an Assistant Professor in L.B.H.S.S. T's I.C.A. Bandra E since 2007.