A Study About Cyber Crimes And Cyber Law In India

Krishna Kumar[1]
Department of Computer Science And Engineering,
Poornima Institute of Engineering & Technology,Jaipur
Dr. Praveen Gupta[2]
Professor, Department of Computer Science And Engineering,
Poornima Institute of Engineering & Technology,Jaipur

Abstract: Crime has been thriving around us since the beginning of the human civilization. Over the ages weapons used to commit crime has grown more sophisticated. With the introduction of computers and internet, the crime enterprise got new area to thrive in the form of cyber crime. Criminals have always done their best to use new technology to their advantages and the rapid development of new digital technology and online markets has provided the criminal entrepreneur with as much opportunity for innovation as their legitimate counterpart.

Keywords: Cyber Laws in India, Cyber Crime, Cyber Security, Hacking, Fraud, Finance, IT Acts

1. INTRODUCTION

Internet has become an integral part of today's life. Computers have made our life a lot easier. It is being used for various purpose such as banking, finance, education, government projects and purposes starting from individual to large organizations. People uses internet to get information related to banking, e-commerce, weather forecasts, business deals, fitness tips, entertainment etc. Upload, download and share are daily routine of people now-a-days. It is estimated that by 2020, there are going to be 666.4million internet users in India (www.statista.com). Technologies are developed for the better of the mankind, but some people use them for negative purpose. Same has happened with internet and computer technology. Many computer users are utilizing computers for illegal purpose such as hacking, banking fraud, spying, data stealing and many more. These are known as Cyber crime. According to Techopedia, Cyber crime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). It is used as a medium to access personal information, business secrets, or uses internet for exploitative purpose. Cyber crime in India increased at a rate of 300 percent from 2011 to 2014. There were 11,592 cyber crime related cases registered in India in 2015. We can define Cyber Law a legal system issued by the governing body to tackle the increasing cyber crime and govern cyberspace. Lack of awareness about such technology among people would end up in a severe damage on finance, moral, emotional or ethical grounds. This paper focuses on to find if people are aware about cyber crimes and cyber laws. If yes, then up to what extent. If no then what steps and measures can be taken by the government and NGOs to make people aware about this issue. This paper aims at making people know about various cyber crimes and cyber law in India.

2. CYBER CRIME AND CYBER LAW

2.1 Classification of cyber crime

Cyber crime can be broadly classified into four major categories which are mentioned below :-

a) Cyber crime against Individual

These are the crimes carried against some individual. Some of them are

Email spoofing which means message appears to be received from some different source other than actual source.

Spamming which are basically junk mails, multiple copies of unsolicited emails.

Cyber defamation uses cyber space to dilute someone's reputation

Phishing is similar to masquerading in which sensitive information such as password, account number, username, credit card number etc. are obtained by disguising as a trustworthy entity.

b) Cyber crime against property

Credit card fraud, Software piracy, Copyright infringement, Trademark violations, Theft of computer source code and many more

c) Cybercrime against Organization

These are the cybercrime which are done against some sort of associations.

Unauthorized accessing of data and changing/deleting them

Denial of Service which is caused when internet if flooded with continuous bogus request to crash the server

Virus attack in which a computer program is designed to infect other computers.

Email Bombing in which server crashes due to lager number of arriving mails.

Logic bomb is an event driven program which crashes computers as soon as the required event occurs.

Data diddling alters raw data just before it is being processed.

d) Crime against society

Some of the cyber crimes done against society are forgery, cyber terrorism, web jacking etc.

2.2 Cyber Law in India

Cyber Law is regulated by governing body in order to put cyber space under check. The abuse of computers are addressed by the Information Technology Act, 2000 (**IT Act, 2000**). It is the primary law in India dealing with cyber crime. It is based on the *United Nations Model Law on Electronic Commerce 1996* (UNCITRAL Model) recommended by the General Assembly of United Nations by a resolution dated 30 January 1997. The original Act contained 94 sections, divided in 13 chapters and 4 schedules. It gave recognition to electronic records and digital signature. A major amendment was made in 2008. It introduced section 66A for offensive messages, section 69 to give authorities the power of "interception or monitoring or decryption of any information through any computer resource".

Some of the sections under IT Act, 2000 are mentioned below:-

Section 65 – Tempering with computer source

If someone intentionally destroy or make someone to destroy/alter computer code used for computer

Penalty: - Someone, if is found guilty, could be jailed for 3 years or/and with fine up to Rs. 200,000

Section 66 – Hacking

If someone intentionally cause loss or damage to the public or destroys any information residing inside computer.

Penalty: - Someone, if is found guilty, could be jailed for 3 years or/and with fine up to Rs. 500,000

Section 66B – Wrongfully receiving stolen computer or communication devices

If someone retains a computer resource which is known to be stolen.

Penalty: - Someone, if is found guilty, could be jailed for 3 years or/and with fine up to Rs. 100,000

Section 66C – Unauthorized use of someone else password

If someone intentionally uses password, digital signature or other unique identification of another person

Penalty: - Someone, if is found guilty, could be jailed for 3 years or/and with fine up to Rs. 100,000

Section 66D – Using computer resources to cheat

If someone cheats somebody with the help of computer resources by personating them over communication devices.

Penalty: - Someone, if is found guilty, could be jailed for 3 years or/and with fine up to Rs. 100,000

Section 66E – Violation of privacy

If someone intentionally captures, publishes or transmits the image of private area of a person without their permission.

Penalty: - Someone, if is found guilty, could be jailed for 3 years or/and with fine up to Rs. 200,000

Section 66F – Cyber terrorism

If someone intentionally uses computer resources to threaten the unity, integrity, sovereignty or security of India.

Penalty: - Lifetime imprisonment

Section 67 – Publishing obscene information

Publishing or transmitting of material containing sexually explicit act, etc. in electronic form.

Penalty: - Someone, if is found guilty, could be jailed for 5 years or/and with fine up to Rs. 10,00,000

Section 67A – Publishing obscene information

Publishing or transmitting of image containing sexually explicit act, etc. in electronic form.

Penalty: - Someone, if is found guilty, could be jailed for 5 years or/and with fine up to Rs. 10,00,000.

Section 67B – Publishing obscene information

Publishing or transmitting of material containing images of child in sexually explicit act, etc. in electronic form.

Penalty: - Someone, if is found guilty, could be jailed for 5 years or/and with fine up to Rs. 10,00,000

Section 68 – Failure to comply with orders

If someone intentionally fails to comply with orders

Penalty: - Someone, if is found guilty, could be jailed up to 3 years or/and with fine up to Rs. 2,00,000

Section 69– Failure/Refusal to decrypt data

If someone fails to provide support to decrypt some message which governing body considers important to maintain the unity, integrity, sovereignty or security of India.

Penalty: - Someone, if is found guilty, could be jailed up to 7 years and possible fine

Section 70 – Attempt to access a protected system

If someone makes attempt to access a protected system.

Penalty: - Someone, if is found guilty, could be jailed up to 10 years and possible fine

Section 71 – Misrepresentation

If someone obtain any license or digital signature certificate using misrepresentation to the Controller or the Certifying Authority

Penalty: - Someone, if found guilty, could be jailed up to 3 years and/or fine up to Rs1,00,000

3. CASE STUDY

SIM Swap Fraud

In August 2018, two men were arrested from Navi Mumbai who were involved in activity of money transfer from bank accounts of many people by getting their SIM card information through illegal means. After getting information they were blocking their SIM cards with fake documents after which they were carrying out transactions. They were accused of transferring 4 crores Indian Rupees. They even attempt to hack a couple of companies.

Cyber Attack on Cosmos Bank

Nearly 94 crores Indian rupees were stolen during a cyber attack which was carried in August 2018 on Cosmos's Bank Pune Branch. The money was transferred to Hong Kong situated bank. Details of debit card holders were obtained by hacking the ATM server of the bank. The centralized banking solution of Cosmos bank was not attacked by the attackers. The balance and the accounts statistics were not changed and the account of holder was having no effect. The switching system which acts as interacting module between the payments gateways and the banks centralized solution was attacked. Numerous wrong message were raised as malware attacked the switching system. 14000 transactions were created with over 450 cards across 28 countries. It was first attack in India on switching system which broke communication between payment gateways and banks.

Website Hacked

Between the months of April 2017 and January 2018, over 22000 websites were hacked as per the report by the Indian Computer Emergency Response Team. The attacks were carried out in order to get information about the services and details of users in their network.

Blue Whale Challenge

The Blue Whale game was an online "suicidal game" targeted at teenagers and had 50 tasks over 50 days with committing suicide as the final task on the list. The game caused numerous suicide around the world including some cases in India.

Some of the task were such as "Wake up in the middle of the night" or "watch a scary movie". As the day passes the game grew more and more sinister and included tasks such as "cut a whale into your arm", "stand on the edge of a building"

WannaCry Ransomware

It is considered as one of the biggest cyber attacks in the history which was carried around the world in May, 2017 including India. Its main target was enterprises and organizations. It infected computers running on older version of Microsoft OS such as XP. The ransomware locked the user's device and prevented them from accessing data and software until a certain ransom was paid which was $300in cryptocurrencies like Bitcoin as per some reports.

BSNL Malware attack

BSNL broadband network in Karnataka sector was greatly affected by a virus which affected 60,000 modems with default "admin-admin" username/password combination. The infected modems were not able to connect to internet. After this, BSNL had issued a notice for the user to replace their default username and password with a new one.

Zomato Hack

One of the largest restaurant aggregation in India, Zomato was hacked and some of its user's accounts were being sold on dark web. Users were lucky that they didn't faced any financial loss since Zomato stores users' information at a separate location.

4. PRECAUTIONS AND SUGGESTIONS

Following are the precautions people should follow to safeguard themselves from potential cyber attacks.

1. Install, use and regularly update antivirus and antispyware software.
2. Use a firewall for internet connection.
3. Download and install software updates for your operating system and application as they become available.
4. Always maintain backups of your data.
5. Make your Wi-Fi networks as secure as possible.
6. Regularly change passwords.
7. Don't share your account information with anyone.
8. Personal and private information on social media should be kept locked.
9. Be updates on major security breaches.
10. Always use two-factor authentication.
11. Have different password for each accounts.
12. Software should be downloaded from authenticated sites.
13. Awareness should be spread on topics such as
    - Ethical use of internet
    - Internet security and its importance
    - Cyber law
    - Technology and their drawbacks
    - Requirements to protect data from being stolen
14. Government should collaborate with ethical hackers to bring out more practical solution for cyber attack.
15. More awareness campaigns should be carried out by governments and NGOs to spread awareness

5. CONCLUSION

Over the ages as the technology has developed the crimes committed using them has also increased significantly. The ways for committing crime has become more and more sophisticated. Cyber crime has been causing more and more personal and financial as well as political losses. So protection against cyber crime is important aspect which is needed to be covered more practically and effectively. IT act, 2000 is an important step taken by the government to regulate the cyberspace. Awareness program should also be conducted. Main purpose of this paper is to spread the content of cyber crime and cyber law to people.

REFERENCES

[1] Ritu Sharma, Yogesh Chaba, Yudhvir Singh, "Analysis in Security Protocol in Wireless ensor Network", Int. J. Advanced Networking and Applications, Volume: 02, Issue: 03, Pages: 707-713 (2010)

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey", Computer Networks Journal, Elsevier Science, Vol. 38, No. 4, pp 393– 422, March 2002.

[3] Umesh Sehgal & Dinesh Kumar," WIRELESS NETWORK SECURITY THREATS", International Journal of Information Technology and Knowledge Management January June 2009, Volume 2, No. 1, pp. 181-183

[4] Anuraj Singh," Studies Report on Cyber Law in India & Cybercrime Security", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 6, June 2017

[5] Anuranjan Misra," A comprehensive legal framework of Indian Cyber Laws", SPC ERA International Journal of Law and Governance Vol.1, No.1 2013

[6] Jigar Shah," A Study of Awareness About Cyber Laws for Indian Youth", International Journal of Trend in Scientific Research and Development, Volume 1(1)

[7] R. M. Kamble, " CYBER LAW AND INFORMATION TECHNOLOGY", International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013 789 ISSN 2229-5518

[8] Animesh Sarmah, Roshmi Sarmah , Amlan Jyoti Baruah," A brief study on Cyber Crime and Cyber Law's of India", International Research Journal of Engineering and Technology (IRJET)