IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A STUDY ON TYPES OF CYBER CRIMES AND CYBER ATTACKS IN INDIA

[1]Bhavika Pandita Hakhroo

[1]Student

[1]Symbiosis Centre for Management Studies, Pune, India

Abstract: With the ever growing increase in the technological revolution in our world , with these opportunities comes the threat of the cyber world. The aim of this study is to understand the types of cybercrimes and cyber-attacks in India. The Information Technology Act has had a significant impact on dealings with crimes related to the cyber / virtual world. The cyber crime rate in India has been increasing. To understand cybercrime, an understanding of the types of cyber crimes is crucial. The preventive measures are necessary to safeguard against the nature of these crimes. It is important to undertake preventive measures and safeguard yourself beforehand and be aware of these types of crimes. The basic measure to prevent cybercrime are to ensure regular computer updates, keep strong passwords and to avoid using public wifi networks

Index Terms **-** Cyber Crime, Cyber Crime Types, Cyber Attacks

I. INTRODUCTION

The Information Technology Act, 2000 (also known as ITA-2000, or the IT Act) is an Act of the Indian Parliament notified on 17 October 2000. It is the law in India in context with cybercrime. One of the major amendments to the IT Law was made in 2008. The Information Technology Amendment Act 2008 is an addition to the ITA Act 2000, changes in the amendment was done taking into consideration the increase in the different type of cybercrimes due to rapid increase in the usage of internet and computers. Cyber crime in India has been growing at an increasing rate and India ranks high among those countries which are victims of cybercrimes. Cyber crime involves an act where a computer as a device has been used for committing the crime. In todays world with India as a developing country the access to internet and computers has increased since the past decade, and more so with it, it brings the vulnerability one can face in the online world. It is the nature of the cyber crimes which makes it borderless and gives the opportunity to cyber criminals to commit their crimes while not even being physically present in the place where the cyber attack has taken place. To understand and safeguard oneself against the nature of these crimes, one must also take preventative measures.

The Government of India, Ministry of has launched the National Cyber Crime Reporting Portal under the National Mission. The portal also provides an opportunity for cybercrime volunteering as a national fight together against cybercrime. It also provides information regarding cybercrimes.

The scenario of cybercrime in India is changing rapidly hence this research was done to better understand cyber crime as a whole and the kinds of attacks which an individual or an organisation can be susceptible to in the cyber world.

II. RESEARCH OBJECTIVES

2.1 To understand types of cyber crimes.

2.2 To understand types of cyber attacks.

III. LITREATURE REVIEW

Juneed Iqbal and Bilal Maqbool Beigh in their research on the trends and challenges in cybercrime mention how India is largely transforming towards a future of ‘Digital India’ in which the dependance of India on the internet increases. This also makes India open to the vulnerability which comes with going digital. The authors state how cybercrime is a global concern. Cybercrimes is the type of crime which can be committed with ease and with no geographical boundaries. Cyber threats can damage systems which are digital , connected to the internet. Subsequently the multifold growth in the domain of internet usage with substantial increases in the number of cybercrime cases along with the global nature and a framework of the laws in India regarding cybercrime. [1]**.**

The number of people who use the internet today are far more than what it was back in the 1990’s. The increase in the number of internet users have facilitated the people with an ease of getting access and sharing of information. The cyber world does not restrict any user as it does in the physical world, as they can freely transact on the world of the internet. Cyber-crime can be understood in the narrow sense and a broader sense as stated by the author these mean computer crimes and computer related crimes respectively [2].

In the paper by Mukta Martolia and Divya, steps to identify a crime when it comes to the cyber world are stated which provide an insight into the functioning of the cyber world crimes and how security of evidence, reporting of evidence and extracting information is evaluated and done. The authors state the types of cybercrimes, the cyber frauds and cyber landscapes [3].

In the study by Yougal Joshi and Anand Singh, the authors state how the online world provides a virtual identity to the criminal. The aspects of cybercrimes range from technological aspect to anthropological aspects and strategic aspect to it. The impact of cybercrime can be of positive and negative developments. The cybercrimes can be committed against individuals in by computers as a target as home use PC use has grown wildly. The attacks of cybercrime can be of three types as discussed in the paper - Attacks on Electronic Identity, Attacks on Minor, Attacks on infrastructure [4].

The study by research scholars identifies factors which will enable facilitation of charge sheeting of cybercrimes in India. The authors give the overview of cybercrime and prevention. The model can be implemented and help in assistance with an objective to identify importance of various variables that could lead to charge sheeting of the accused. The study and the model in the study can guide authorities in focusing on relevant information related to cybercrimes. This helps in improving the efficiency of the people authoritative in solving crimes related to the cyber world. The study was done in cybercrimes reported in Karnataka as one of the subsets and the other as the rest of Indian states [5].

In the research done by Tanya Syngle on an overview of corporate cybercrime in India , we get an understanding of the nature of the cyber-attacks which take place across US and India. The author states the frequency of more than 70 percent in cyber-attacks within a 12-month period in both the countries. The profile of the cyber minds, the nature of the cyber-attacks all play a very pivotal role in understanding cybercrime. Computers in our day to day life is integrated with us through one or the other direct or indirect medium [6]**.**

The study by Ms. Babita Banga and Mr. Tarun Tiwari on cybercrime in India and how cyber can be a domain of war and terror , the NSA leak revealing the spying on India by various agencies is one such case as mentioned in the study. Currently Cyber is the fifth and the new domain of warfare. According to the study India being one of the biggest IT nations, is open to threats on cyber security from across the globe [7].

IV. RESEARCH METHODOLOGY

The research was done primarily by gathering secondary data. The research was done by acquiring data through secondary sources including websites, journals, articles, surveys, reports.

V. DISCUSSION

5.1 Types of Cyber Crime and Cyber Attacks

1. Cyber stalking – Cyber Stalking in general words means the use of computer systems and digital mode of communications for attempting to advance a personal interaction constantly even after a clear message of disinterest by the person, this also involves online harassment , defamation, slander.

2. Intellectual Property Crimes – Also known as IPR , Intellectual property rights consist of a lot of rights , IPR includes Copyright, Patents, Trademark, Trade secrets. Intellectual Property Law encourages the creation and protection of a wide variety of intellectual goods. The common Intellectual Property Rights violations are counterfeit, piracy - infringement, also stealing stealing artistic and literary works and designs comes under this.

3. Bot Networks - Botnet is a combination of the words robot and network, Botnets include a number of devices connected by the internet which allows the hacker to control them simultaneously. They are used to perform Distributed Denial-of-Service (also known as DDos) attacks.

4. Transmitting Virus – Viruses are programs which attach themselves on a computer and can be circulated within the computer , these viruses can copy information from the computer system under siege and use it for various unlawful purposes. There are different types of viruses , stealth viruses , polymorphic virus, fast and slow infectors.

5. Hacking – Hacking refers to activities which can attempt to enter a computer network by unauthorised access , this includes putting malicious content on your device (computer, laptop, smartphone , Tablet). Another type of hacking is those who are politically motivated known as hacktivists. There are white hat, grey hat and white hat hackers

6. Internet Time Thefts – Internet Time Theft is another type of hacking in which a hacker gets access to your Internet Services and ID passwords for the same without the knowledge of the person whose paying for those internet hours.

7. Cracking – Cracking in general words means to get into a computer illegitimately to steal data, view sensitive information. A cracker is different from a hacker because he uses backdoors in a program and then use that backdoor to gain access. Whereas a hacker uses extensive computer knowledge and logic to bypass security.

8. Phishing – Phishing is the type of fraud that involves stealing information related to your banking account card details via email.

9. Vishing (Voice Phishing) – Banking account card information is taken by the fraudsters through telephonic means.

10. Carding – It is the type of fraud which uses stolen credit cards to make payments for criminal activities or illegal activities without the knowledge of the owner of the credit card , it is also known as credit card trafficking.

11. E-Mail/SMS Spoofing – Email spoofing is an email sent by an address which is not valid or is forged under the pretext of someone else (is fake), this email is then used to mislead the recipient or make false statements and dig out info.

12. Cross-site Scripting – In cross site scripting the attacker executes malicious cripts o the website / the web browser, so that when anyone visits that site the actual attack occurs then, this allows the malicious script to reach the visitors browser.

13. Cyber Squatting- It is the attempt of using an internet domain name, or using the name of a brand and use it to the advantage of personal gain. It is an attempt of representing a brand online without due permission or consent.

14. Child Pornography– Child Sexually Abusive Material (CSAM) is the reference to images or videos which contain sexually explicit content of child being abused or exploited. Section 67 (B) of IT Act states that “it is punishable for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form.

15. Online Sextortion – It is threatening someone with the context of distributing or sharing private information using an electronic medium incase the victim does not provide sexual favours.

16. Sexting – Sexting is the act in which a cell phone is used to send sexual images, videos texts.

17. Cyber Grooming – Cyber grooming is an act in which a person develops a relationship online with a young person and forces them into doing sexual act.

18. Invasion of Privacy – All the activities which an individual does on the cyber space if comes under surveillance by anyone is a threat to anyone the information of the individual

19. Cyber Vandalism – Cyber vandalism is the destruction and damage taking place in the cyber space, it can be done by creating a malware which stops te functioning of a computer system, or deface any website online.

20. Cyber Trespass – Cyber trespassing is accessing unauthorised computer infrastructures and obtaining information from the protected computers.

21. Cyber Bullying – When electronic mediums like laptops, mobile phones, laptops are used to harass or bully an individual.

22. Crypto jacking – It is malicious crypto mining an online threat in which a mobile or computer device systems and mine online forms of money known as cryptocurrencies.

23. Cyber Trafficking – Advertising of victim’s services online on the internet and also advertising and recruiting victims through cyberspace is known as cyber trafficking.

24. Key Logger – It an act of crime in which the keyboard activity of an individual is recorded without their awareness.

25. Identity Theft – Impersonating to be someone else on the internet or creating a fake identity and then acquiring information from an individual is known as identity theft.

26. Website Defacement – It the act of defaming, changing the graphics of a website, and posting vulgar images and messages on the website.

27. Evil Twin – An evil twin is a wifi point access which looks legitimate but is instead used for obtaining information through wireless communication

28. Online Drug Trafficking – When drugs such as heroin, cocaine, marijuana are sold illegally with the use of electronic means it is known as online drug trafficking.

29. Espionage – It is the act of accessing data and information without the owner of the data and information by neither being made aware about it nor by seeking permission of the owner. Here the data and information can be of government or other organisation.

30. Online Job Fraud – This is an attempt to fraud people under the false pretext of providing them with employment with a wage using means of internet.

PRACTICES FOR PREVENTION OF CYBER CRIME

1. Passwords - One of the basic measures for prevention of cyber crime is to keep strong passwords for your online accounts, make passwords are not too obvious like the name of a pet , or your husband / wife/ child, or your birthdate. Keep updating your passwords at regular intervals.
2. Wireless Networks - Avoid using wireless networks which are available at public spaces such as cafes, stations. Ensure that your wifi networks at home are WPA certified.
3. Computer Updates- Update your computer systems, mobile operating systems as regularly as possible, these updates on the operating systems throws off many hackers as updates have built in programs to block and detect attacks.

VI. CONCLUSION

The future of the cyber world and its impact on our daily lives is increasing everyday, our dependence on the internet and computer systems makes us more vulnerable and susceptible to these different types of cyber crimes including cyber frauds, cyber bullying, cyber grooming. In this study 30 cyber crimes and types of cyber attacks were studied, and the basic preventive measures to protect oneself against such cyber-attacks were listed. We need to be more aware and attentive when it comes to cyber crimes as these crimes are borderless and can happen even in the dead of the night when an individual might be fast asleep, whereas a hacker in some other part of the world might be planning to hack and steal your financial information, hence it is important to undertake preventive measures and safeguard yourself beforehand and be aware of these types of crimes. The study also lays emphasis on the importance of understanding these types of crimes and how to have an understanding to ensure that as an individual one can recognise these threats. The basic measures to prevent cyber-crime are to ensure regular computer updates, keep strong passwords and to avoid using public wifi networks. These types of cyber crimes also nod the direction towards the eminent importance of cyber security, in the near future. The future scope of the research can be towards understanding these types of threats and then how to make the cyberspace a more protective and secure sphere. The importance of computer systems is very necessary.

VII. REFRENCES

[1] J. Iqbal and B. Maqbool Beigh, "Cybercrime in India: Trends and Challenges," *International Journal of Innovations & Advancement in Computer Science,* vol. 6, no. 12, 2017 December 2017.

[2] V. Kandpal and R. Singh, "Latest Face of Cybercrime and Its Prevention In India," *International Journal of Basic and Applied Sciences,* vol. 2, no. 4, pp. 150-156, 2013.

[3] M. Martolia and Divya, "Types of Cybercrime in India and Its Detection," vol. 7, no. 9, Joural of Critical Reviews 2020.

[4] Y. Joshi and A. Singh, "A Study on Cyber Crime and Security Scenario in INDIA," *International Journal of Engineering and Management Research,* pp. 13-18, 2013.

[5] A. S. N. Murthy, V. Nagadevara and R. De, "Predictive Models in Cybercrime Investigation : An application of Data Mining Techniques," *International Journal of Information Systems in the Service Sector,* vol. 2, no. 3, pp. 1-12, September 2012.

[6] T. Syngle, "An Overview of Corporate Cybercrime in India and US," *International Journal of Cyber-Security and Digital Forensic,* vol. 6, no. 2, pp. 49-59, August 2017.

[7] B. Banga and T. Tiwari, "Cybercrime in India : Types and Target of Cyber Attack," *International journal of Science Technology & Management.*