IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cyber Crime Investigation In India Vs. Australia

Manisha Guleria

Research Scholar

Department of Police Administration

Panjab University Chandigarh

ABSTRACT

The internet is the essence of life in the 21st century. With the development in technology, the internet has become more intertwined with our lives than we can think of. Cyber Security plays an important role in the field of information technology. Securing the information has become one of the biggest challenges in the present day. Nowadays when people think about cyber security, the next thing that comes to their mind is cybercrimes, which have increased massively day to day. Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device. Cybercrime is a serious threat nowadays. The paper examines the various forms of cybercrimes, cybercrimes in India and Australia. It also includes cybercrimes from the aspect of international laws and Cyber Security Measures for Organizations to Prevent Cyber Attacks.

OBJECTIVES:

- To. Understand the concept of cyber-crime
- To study cyber-crime in India and Australia

METHODOLOGY

In this research paper the data for the present study is collected mainly through secondary sources the objectivity of historical and current writings has been used to develop a frame work of the study and to arrive at an unbiased conclusion.

INTRODUCTION

The role of the internet's global significance has enhanced and its impact is enormous. The impact of the internet is growing and has increased the opportunities for in almost all the fields, including sports, education, employment, entertainment, etc. The impact of digital space has played a vital role in individual's lives in today's 21st century. The digital space has both advantages and disadvantages. Every crime has its impact on the nation, society and the world. In the same way, the impact of cybercrimes on the society, nation, and individual is massive. Cybercrime is any illegal activity which is committed through a computer network, the internet. Cyber-crime involves the interruption of privacy, or damage to the computer system properties such as files, website pages or software. Cybercrime is any criminal activity involving computers and networks. It includes fraud, email spams, theft of government or corporate secrets through criminal trespass, defamation etc. Cybercrime includes anything from copying illegal music files to theft of millions of dollars from online bank accounts. Cybercrime also includes non-monetary offenses, such as creating viruses on other computers or posting confidential business information on the Internet (Anisha2017).

REVIEW OF RELATED LITERATURE:

Animesh Sarmahand and Amlan Jyoti Baruah (2017) the authors of this article claim that criminal activities or Internet related offenses / crimes are called cybercrime. To stop or punish cyber criminals, the term "Cyber Law" has been introduced. The authors believe that cyber law is the part of legal systems that deals with the Internet, cyberspace and legal issues. It covers a large area, covering many secondary topics, as well as freedom of expression, Internet access and use and online security or online privacy. It is generally referred to as web law. The primary goal of the author when writing this document was to spread the content of cybercrime among ordinary people. At the end of the document "A Brief Study on Cyber Crime and Cyber Laws in India", the authors said that cybercrime can never be recognized. If someone falls into the cyber-attack dam, file and register a case at the nearest police station. If criminals are not punished for their actions, they will never stop.

IAMAI (2021) a report published by Internet and Mobile Association of India, on internet usage in India, about 67% of the users are male compared to which only 33% are female. This disparity between the male and female users is the major reason for the growth of cybercrime incidents against women.

WHAT IS CYBER CRIME?

Cybercrimes can be defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including chat rooms, emails, notice boards and groups) and mobile phones".

Cyber-crime involves the use of internet and computer. It threatens an individual's privacy by disclosing or publishing their personal or confidential information online with the aim of degrading their reputation and causing them physical or mental harm either directly or indirectly. Women are generally the targets of these offenders because they are inexperienced and lack knowledge of the cyber world, thereby falling prey to the technological fancies.

TYPES OF CYBER-CRIME

Hacking - hacking is an act committed by an impostor by reading other's computer system without their permission. Hackers are computer programmers, who have an innovative understanding of computers and commonly misuse this knowledge for deceitful reasons. They have excess skills in a particular program or language and they are excelled in the internet space. A hacker breaks into systems to steal personal banking information, a corporation's financial data, etc. They also try to alter systems so that they can complete tasks at their urges. These people are called as black hat.

Virus dissemination: computer programs that infect a system or files, and have a inclination to circulate to other computers on a network. They disrupt the computer operation and affect the data stored either by altering it or by deleting it.

Phishing is done by removing confidential information such as credit card numbers and username passwords by representing themselves as a authentic enterprise. It is carried out by email bluffing. Phishing is not only done through emails or websites, but also through phone calls.

Cyber stalking is when a person is tracked or followed online. A cyber stalker doesn't physically follow the victim directly but he virtually follows the stalkee online and harasses him or her and makes threat using verbal coercion. It's an infringement of one's online privacy. Maximum victims of this crime are women who are stalked by men and children who are stalked by adult predators.

Identity Theft and Credit Card Fraud identity theft is when someone steals other's identity and pretends to be them to access to resources such as credit cards, bank accounts and other profits in their name. The fraud may even use that identity to commit other crimes.

Software Piracy is the utmost common crime which most of the people intentional or unintentionally commit. It is an illegal use and distribution of computer software. Software developers develop these programs, and piracy limits their ability to make enough profits to sustain application development. This affects the global economy in whole as funds are transmitted from other sectors which results in less investment in marketing and research.

Cloning means where one's ideas are copied and does not give their reference. It is a copyright infringement. Other cybercrimes including **internet fraud, cyber bullying, child pornography**

CYBER-CRIME IN INDIA

According to Cyber Threat Report of 2019: 69% of Firms Face Serious Cyber Attacks in India! Do you know that India is in has been ranked the second position amongst the countries affected by cyber-attacks from between 2016-2018? According to a source, there was a 22% rise in cyber-attack in India on IT deployments. India has faced the most number of attacks in the IT department this year. In fact, India has been consecutively facing cyber-attacks, the second time in the row! In a recent study, it was revealed that out of 15 Indian cities, Mumbai, New Delhi, and Bengaluru have faced the maximum number of cyber-attacks. In the Annual Cyber Security Report by CISCO, 53% of cyber-attacks caused more than $500K of financial loss to organizations in 2018. India has faced a rise of 7.9% in data breaches since 2017. Also, the average cost per data breach record is mounting to INR 4,552 ($64). Cyber-attacks in India have risen up to such an extent that our country ranks fourth out of the top 10 targeted countries in the world. In a report by India Today, Chennai experienced the highest percentile of cyber-attacks with a stat of 48% in the first quarter of 2019. No survey or warning has brought any change in the cyber security policies of companies across the nation. In spite of witnessing several cyber-attacks in India, people are still not aware of lucrative cyber security solutions to prevent their organization from any other attack.

STEPS TO PREVENT CYBER CRIME IN INDIA:

The Information Technology Act of 2000, together with the Penal Code of India, has adequate provisions to deal with prevailing computer crimes. It provides for penalties in the form of imprisonment ranging from two years to life imprisonment and fines / penalties depending on the type of cyber-crime.

However, the government has taken the following measures to prevent cybercrime:

- The cybercrime cells were established in the States and territories of the Union to report and investigate cases of cybercrime.
- The government has set up IT research and forensic training laboratories in the states of Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Meghalaya, Manipur and Jammu and Kashmir for the training of the police and the judiciary in these states.
- In collaboration with the Data Security Council of India (DSCI), NASSCOM, Cyber Forensic Labs were established in Mumbai, Bangalore, Pune and Calcutta for awareness and training.
- Cybercrime investigation programs. National Law School, Bangaluru and NALSAR University of Law, Hyderabad, are also involved in conducting various awareness-raising and training programs on law and cybercrime for court officials.

CYBER-CRIME IN AUSTRALIA

The Australian Cybercrime Online Reporting Network (ACORN) recorded 39,491 cybercrime incidents in 2015; its first year of operation (ACORN 2016). Australian Federal Police (AFP) Commander David McLean reported that, in one month alone, over 3,500 people had contacted police about perceived cyber-crimes. He added that these cyber threats were “typically classified as being state-sponsored or criminally-motivated” (Duffy 2015). Such incidents appear to be on the rise. Fraud and scams were the most reported type of cybercrime incidents reported to police. About two in five victims were aged between 20 and 40. Social Network Sites (SNS) were a significant vector for cybercrime offences (ACSC 2015). Annual losses were estimated to be aboutAUD1 billion; mostly from credit card fraud and scams many of which originated online. Data from the ABS (2016) Personal Fraud Survey also confirm these trends, with 1.6 million Australians reportedly being a victim of personal fraud and 126,300 being victims of identity theft. Just over half of the Australian population aged 15 and over were exposed to at least one scam, and 4 percent of these were victimised, either due to supplying personal information, money, or both.

The Australian Cyber Security Centre’s 2015 Threat Report (ACSC 2015) highlights the emergence of cybercrime-as-a-service, introducing new business models to cybercriminals, and increasing their spread and sophistication. The FBI Cybercrime Division prosecutor Gavin Corn (GIN 2014) observed enhanced networking among criminal groups: “Cybercrime wasn’t even a part of organized crime before, and now it’s the epitome of it”, including a rapid uptake of encrypted and anonymised technology such as re-routing systems that hide the location of internet connections and servers allowing “anonymous payment systems like Bit-coin” As at November 2015, there were about 21 million Australian internet users and 14 million

As at November 2015, there were about 21 million Australian internet users and 14 million Australian Facebook users; that is 93 and 73 percent of the total population respectively (Mini watts 2015). The IT, combined with more businesses using social media, will increase the range and scale of cybercrime threat vectors, as new vulnerabilities in social network services arise.

AUSTRALIAN CYBERCRIME PROTECTION

1. **ACORN: Australia** government has set up of online reporting network of consumer **intelligences** to report and cybercrime or new threat that affects Australians if not. It is an agency that delivers national plan to combat cybercrime. It acts as online resilience to cybercrime where public and organisation can online report cybercrime securely. It acts as club of national agencies and territory governance.

2. **ACSC**: Australia Cybercrime security centre defines various frameworks and guidelines in order to protect assets of organisation to avoid risks and threats. It gives industries enterprise risk management assurance and public-private hub for information sharing. It responds cyber threats to **CERT** (Computer emergency and response team).It works together with government, industry and Australians to increase

cybercrime awareness at maximum. It basically works in collective mode with department of home affairs whenever tracing out new government policy against cybercrime.

INTERNATIONAL COOPERATION

The suppression of internet-driven CEM is a major challenge for law enforcement agencies across the globe. However, effective alliances have been formed across nations to share intelligence and prosecute the most serious offences. The Virtual Global Taskforce coordinates responses to multinational exploitation cases. It was established in 2003 to help respond to and investigate serious CEM cross-border cases. Over 1,000 investigations have been completed to date. The AFP and state police are actively engaged in this work, often in collaboration with the FBI’s Violent Crimes against Children (VCAC) unit, and agencies in Italy, the UK, Canada, and Saudi Arabia. Many cyber security regulatory frameworks have emerged around the world to address the problems of cybercrime. They vary from state-centric approaches to volunteer groups or alliances that foster cross-national government, industry, and academia collaboration. Non-profit groups such as Spamhaus and Virus Total provide critically important services. Emblematic of this movement is the US National Institute for Standards and Technology (NIST) Cyber security Framework — that regularly updates cyber security best practices and has been influential in shaping the effectiveness of cyber security in the US, Canada, India, and Australia (Shackelford, Russell, and Haut, 2016). Other efforts have been undertaken against CEM, scams, and fraud. For example, the London Action Group tackles spam; and the Phish Tank is an anti-phishing clearing house associated with Open DNS and the Anti-Phishing Working Group (APWG). The APWG—a global consortium of industry, academia, and law enforcement—tracks the prevalence and scope of phishing attacks, coordinates responses to phishing, and advises governments and industry. These are some of the examples of the role NGOs can play in the mitigation of cybercrime and the pluralism that is essential in the partnerships needed for effective prevention.

PREVENTIONS

- Use strong passwords: Don‘t repeat your passwords on different sites, and change your passwords regularly. Make them complex. That means using a combination of at least 10 letters, numbers, and symbols. A password management application can help you to keep your passwords locked down.
- Keep your software updated: This is especially important with your operating systems and internet security software. Cybercriminals frequently use known exploits, or flaws, in your software to gain access to your system. Patching those exploits and flaws can make it less likely that you‘ll become a cybercrime target.
- Manage your social media settings: Keep your personal and private information locked down. Social engineering cybercriminals can often get your personal information with just a few data points, so the less you share publicly, the better. For instance, if you post your pet‘s name or reveal your mother‘s maiden name, you might expose the answers to two common security questions.
- Strengthen your home network: It‘s a good idea to start with a strong encryption password as well as a virtual private network. A VPN will encrypt all traffic leaving your devices until it arrives at its destination. If cybercriminals do manage to hack your communication line, they won‘t intercept

anything but encrypted data. It‘s a good idea to use a VPN whenever you a public Wi-Fi network, whether it‘s in a library, café, hotel, or airport.

- Keep an eye on the kids: Just like you‘ll want to talk to your kids about the internet, you‘ll also want to help protect them against identity theft. Identity thieves often target children because their Social Security number and credit histories frequently represent a clean slate. You can help guard against identity theft by being careful when sharing your child‘s personal information. It‘s also smart to know what to look for that might suggest your child‘s identity has been compromised.
- Know what to do if you become a victim: If you believe that you‘ve become a victim of a cybercrime, you need to alert the local police and, in some cases, the FBI and the Federal Trade Commission. This is important even if the crime seems minor. Your report may assist authorities in their investigations or may help to thwart criminals from taking advantage of other people in the future

CONCLUSION

Cybercrimes exist in almost all the countries, and the respective governments are taking measures to safeguard against cybercrimes. Since 2020, due to the covid 19 pandemic, everyone from children to the elders all are dependent on the digital area. And there has been rise in cybercrimes during this period. There are many issues like cyber bullying, defamation, cyber fraud, etc., that has become most common crimes. The reason cybercrimes take place is because of the easy access of the devices, sometimes the negligence of the users. In India, and Australia many people are not be aware of such crimes, and when they are hacked, they suffer losses but they might not know what has happened. So first its very important to be aware of such crimes and their rights in digital space. The Indian government and Australian government have taken methods to prevent cybercrimes in the country, but still there is no end. The government is making sure that the victims are compensated or provided justice.

References

Animesh Sarmahand and Amlan Jyoti Baruah (2017), Volume 04, Issue 06, PP. 1633-1640

Anisha, (April, 2017) Awareness and Strategy to prevent cybercrimes- Indian perspective, vol. VII, INDIAN JOURNAL OF APPLIED RESEARCH,

Australian Cyber Security Centre’s (ACSC) Annual Report 2015, available at (https://www.acsc.gov.au/publications/ACSC_Threat_Report_2015.pdf)

Australian Cybercrime Online Reporting Network (ACORN) 2016, Australian Criminal Intelligence Commission, Canberra, available at https://acorn.govspace.gov.au/resources/).

.Cyber Crime in India: A Comparative Study M. Dasgupta, 2009

India Internet 2019, IAMAI, (Jan 28, 2021), https://cms.iamai.in/Content/ResearchPapers/d3654bcc-002f-4fc7-ab39-e1fbeb00005d.pdf

Internet Resources :

[1] http://en.wikipedia.org/ wiki/Security

[2] http://en.wikipedia.org/wiki/Data_ security

[3] http://en.wikipedia.org/wiki/Information_security

[4] http://en.wikipedia.org/wiki/Computer_ security

[5] http://www.cyberlawclinic.org/casestudy. asp