

Cyber Crime and Its Extent

Aadesh Taneja*

*Student at Saint MSG Glorious International School, Sirsa, Haryana, India

Email: aadesh47taneja@gmail.com

Abstract:

Any crime that uses a computer or network is considered a cybercrime, sometimes known as computer crime. People and businesses are exposed to the expanding hazards of cybercrime as due to their increased reliance on technology. Nowadays, it's pretty typical for us to use computers for daily tasks. For instance, we use personal computers, smartphones, general surfing areas, and other devices to pay our life insurance premiums, and electricity bills, reserve aircraft, train, or bus tickets, order books, and so forth. Since then, the number of people conducting business online has proliferated due to the ease it offers the user to conduct business without being physically present in the region where the transaction occurs. Along with the rise in cybercrime, there are also an increasing number of users doing online transactions. Online users must be aware of these attacks and exercise caution when conducting online transactions due to the rise in cyberattacks. In this context, the paper will review the growth of cybercrimes in India and measures taken by the government of India to combat the crimes.

Keywords —Extent of the crime, IT Act 2000, Cybercrime, Cyberlaw, Cybercrimes in India, Effects caused by cybercrime, Cyber Security

I. INTRODUCTION

The Internet changes everything. It challenges our beliefs about how things ought to work, including how governments ought to be run, how businesses ought to be operated, how teachers ought to instruct students, and even how homemakers ought to create new dishes. It muddles our preconceived notions about what we believe to be true about the world, about one another, and about ourselves. It is simultaneously freeing, thrilling, complex, and terrifying. Most individuals still find the Internet mysterious, intimidating, confusing, and frightening. The Internet has grown tremendously, and with that expansion have come more chances for cybercrime. Since the Internet has spread so quickly over the world, computer crimes have expanded to include not only hacking and cracking but also extortion, fraud, money laundering, software piracy, and corporate

espionage, to mention a few. Law enforcement authorities have expressed frustration over lawmakers' incapacity to keep cybercrime legislation abreast of the rapidly advancing technology landscape. Legislators must strike a balance between the opposing objectives of individual liberties like free expression and privacy and the necessity to preserve the integrity of the world's public and private networks. In sections 2 and 3 of this article, we begin by providing an overview of types of cybercrimes, and their effects. Then in Section 4, we will discuss the extent of it in India, and then in Section 5, we will identify the precautions that we can use to stay away from this crime.

II. TYPES OF CYBERCRIME

- A. Identity Theft: Identity theft, commonly referred to as identity fraud, is a crime where a forger acquires significant pieces of personally identifying information.
- B. Online Scams: Online scams take advantage of their victims by using internet-connected services or software to commit fraud against them or, in some other way, exploit them.
- C. Cyber Stalking: a crime where the perpetrator harasses the victim using electronic messaging, such as email or instant messages, or by posting notices to a website or discussion forum
- D. Illegal Content: Illegal content frequently consists of offensive, hurtful, or manipulative material intended for people who are harmed, most often psychologically.
- E. Unwanted Programs: Despite the likelihood that people downloaded it, a potentially unpleasant program is one that may be unwanted. They are frequently downloaded along with a desired programme by the user.

III. EFFECTS OF THE CRIME

- A. The psychological effects of cyber threats may surpass traditional terrorism, depending on who the attackers and victims are. Online attacks and crimes can cause emotional trauma to victims, which can make them depressed.
- B. It may affect an individual's or a family's financial situation. The report concludes that cybercrime costs nearly \$600 billion annually, or almost 1% of global GDP.

IV. EXTENT OF THE CRIME IN INDIA

India, home to the world's second-largest internet-connected population, was no exception to the growing digital village. Our digital societies are open to new vulnerabilities due to the world wide web's increased connectivity, even though it promises significant progress. Cybercrime has expanded at a rate comparable to emerging technologies and has no boundaries. Cybercrimes were estimated to have cost Indian consumers more than 18 billion dollars in 2017. However, these were only estimates based on the numbers that were

reported. Due to a lack of cybercrime awareness or classification mechanisms, the figures may be under-reported in a country like India. A dedicated online portal for reporting cybercrimes and other recent government initiatives may be to blame for the sudden rise in online crimes beginning in 2017.

Compared to the rest of the country, Uttar Pradesh in the north had cybercrimes, with over six thousand cases filed with the authorities in 2018.

That year, Karnataka, India's tech state, followed suit. The majority of these cases were filed under the IT Act. In 2019, India saw a significant rise in the number of cybercrimes reported. Over 44.5 thousand incidents of cybercrime were recorded that year. During the period that cybercrime was measured, Uttar Pradesh and Karnataka had the most immense proportions.

V. PRECAUTIONS TO BE TAKEN

- A. Never share your OTP/Password to anyone
- B. Scan your device on a regular basis
- C. Never provide your personal information on your social media
- D. Enable 2-factor authentication on your social media handles.

VI. CONCLUSIONS

Although not everyone is a victim of cybercrime, they are still at risk. Computer-based crimes come in all shapes and sizes, and not all take place behind a computer. The identity of the hacker varies from 12 to 67 years old. The victim would not even be aware that they were being hacked because the hacker could reside on three different continents. The problem of the 21st century is crimes committed via computers. Criminals no longer need to rob banks or be outside to commit crimes, technological advancements. Everything they require is in their lap. They no longer have guns as their weapons; They use passwords and mouse cursors to attack. Therefore, you must prepare yourself and adhere to all instructions.

VII. REFERENCES

- [1] <https://rjhsonline.com/HTMLPaper.aspx?Journal=Research%20Journal%20of%20Humanities%20and%20Social%20Sciences;PID=2017-8-4-12>
- [2] <https://www.sciencedirect.com/topics/computer-science/cybercrime>
- [3] <https://legabhyas.com/2022/03/17/important-steps-that-all-cyber-crime-victims-must-take/>
- [4] The Art of Deception: Controlling the Human Element of Security by Kevin Mitnick