A STUDY ON CYBERCRIME: ITS IMPACT AND AWARENESS TOWARDS SOCIETY

Gurjeet Singh Pandher,[1] Rahul Thour[2]

[12]Department of Computer Science & Applications, Desh Bhagat University, Mandi Gobindgarh

ABSTRACT

Cybercrime is criminal activity that targets or uses a computer, network, or connected device. Most cybercrimes are committed by hackers seeking financial gain, though some aim to damage systems for other reasons. As technology evolves, cybercrime and hacking are increasing rapidly. Initially driven by small groups or individuals, cybercrime now involves professional hackers, adolescents aged 6–18, scammers, phishers, malware authors, and spammers. Common cybercrimes in India include credit card fraud, bank robbery, illegal downloads, industrial espionage, child pornography, online scams, cyberterrorism, and virus/spam distribution.

The digital age has made cyberspace borderless, increasing cybercrime globally. In India, the Information Technology Act, 2000, provides the legal framework for combating cybercrime. Continuous updates to cyber laws are necessary to address evolving **threats.**

Keywords: Cyber-Crime, Cyber-Criminals, Awareness, Cybersecurity, Internet, IT Act

INTRODUCTION

Cybercrime can involve using a device as a tool or target for committing crimes, such as malware attacks or cyber-enabled fraud. This study assesses awareness and preparedness among individuals and organizations regarding cyber threats. By identifying knowledge gaps, strategies can be developed to enhance cybersecurity education and foster a culture of vigilance.

This study aims to provide insights into cybercrime forms, societal impact, and recommendations for enhancing cybersecurity awareness.

Cybercrime in the World

- **2018:** 208,456 – 212,485 cases
- **2019:** 394,499 – 1,158,208 cases
- **2020–2021:** 1,402,809 cases

Cybercrime Cases in India

Year	Cases
2022	26, 121
2021	27,248
2020	21,796
2019	12,317
2018	11,592

Types of Cybercrimes

1. **Against Persons:** Harassment via cyberspace, sexual, racial, or religious targeting.
2. **Against Property:** Destruction of property, harmful programs, unauthorized access, data leaks.
3. **Against Government:** Cyberterrorism targeting information exchange or making electronic threats.

Cybercriminals

- **Kids (9–16):** Often unaware, hacking for pride.
- **Organized Hacktivists:** Hackers with political, social, or religious motives.
- **Disgruntled Employees:** Exploit automation and computer systems to harm employers.
- **Professional Hackers:** Ethical or industrial hackers targeting rivals for financial or strategic gain.

LITERATURE REVIEW

- Aparna & Chauhan (2012): Awareness reduces cybercrime; responsibility lies with government and users.
- Mehta & Singh (2013): Male netizens are more aware of cyber laws than females.
- Hasan et al. (2015): Female students in Malaysia were more aware than males.
- Archana Chanuvai Narahari & Vrajesh Shah (2016): Survey of 100 respondents showed partial awareness; need for more education.

Steps to Prevent Cybercrimes

- Keep personal information private.
- Avoid sending photographs to strangers online.
- Do not disclose bank details, OTPs, or documents.
- Avoid unknown websites and apps; use cyber-secured apps.

Impacts of the Study

1. Increased understanding of cybercrime forms and societal implications.

2. Heightened awareness of cybersecurity.
3. Policy development guidance.
4. Behavioral changes towards safer online practices.
5. Empowerment of stakeholders.
6. Economic insights for investment in cybersecurity.
7. Recognition of psychological impacts.
8. Trust-building in digital platforms.
9. Emphasis on education and training.
10. Promotion of international collaboration.

Awareness and Perception

Knowledge gaps and misconceptions exist; education, training, and media shape perceptions. Public awareness campaigns and cybersecurity initiatives are crucial.

Research Methodology

- **Objectives:** Understand respondent education and awareness, measure victimization, internet usage, safety awareness, and experiences.
- **Data Sources:** Primary (survey, questionnaire); Secondary (journals, internet, newspapers).
- **Sample Size:** 50
- **Sample Method:** Descriptive survey

RESULTS AND INTERPRETATION

Table 1 – Awareness about Cybercrime

Category	Number	Percentage
Very well	10	20%
I know about it	13	26%
Not so well	8	16%
Don't know	19	38%
Total	50	100%

Analysis: 38% unaware, 20% very well aware, 16% moderately aware.

Table 2 – Experiences of Cybercrime Situations

Situation	Number	Percentage
Trojan or malware	8	16%
Auto-generated mails	31	62%
Publishing obscure material	2	4%
Confidential reports hacked	2	4%
Never experienced	7	14%

Analysis: Auto-generated mails most common; 14% never experienced any cybercrime.

Table 3 – Victimization

Frequency	Number	Percentage
Never	37	74%
1 time	11	22%
2–5 times	2	4%
More than 5 times	0	0%

Analysis: Majority never victims; 26% experienced cybercrime at least once.

Table 4 - Law Effectiveness Perception

Category	Number	Percentage
Strongly agree	9	18%
Agree	12	24%
Disagree	7	14%
Strongly disagree	18	36%
Neutral	4	8%

Analysis: 36% believe laws are ineffective; only 42% agree/strongly agree laws can control cybercrime.

Findings

- 38% unaware of cybercrime
- 62% experienced auto-generated emails
- 16% experienced malware/Trojans
- 22% experienced cybercrime personally
- 36% strongly disagreed that laws are effective

CONCLUSION

Cybercrime is among the fastest-growing crimes. Awareness and preventive measures are essential. The IT Act, 2000, provides the legal backbone in India. Governments, individuals, and organizations must collaborate to improve cybersecurity awareness, education, and resilience.

REFERENCES

Akdeniz, Y., & Walker, C. (2018). Cybercrime: Key Issues and Debates. Routledge.

Holt, T. J., & Bossler, A. M. (2016). Cybercrime in Progress. Routledge.

Grabosky, P. N. (2016). Cybercrime: The Transformation of Crime in the Information Age. Cambridge University Press.

Jaishankar, K. (Ed.). (2016). Cyber Criminology: Exploring Internet Crimes and Criminal Behavior. CRC Press.

Wall, D. S. (2018). Cybercrime and the Culture of Fear. Information & Communications Technology Law, 27(2), 195-213.

Ruud, J., & Rollins, J. (2019). Cybercrime: A Reference Handbook. ABC-CLIO.

Goodall, G., & Thorsen, E. (2019). Cybercrime and its Victims. Routledge.

Websites:

1. https://www.kaspersky.com/resource-center/threat
2. https://aag-it.com/the-latest-cyber-crime-statistics/
3. https://purplesec.us/resources/cyber-security-statistics/
4. https://us.norton.com/blog/emerging-threats/cybersecurity-statistics