

INVESTIGATING THE IMPACT OF CYBERCRIME FOR AWARENESS

*Divya Sharma

**Dr Atal Kumar

Paper Received: 06.11.2021 / **Paper Accepted:** 04.12.2021 / **Paper Published:** 05.12.2021

Corresponding Author: Divya Sharma; Email: divyasharma260.ds@gmail.com; doi:10.46360/cosmos.mgt.420212020

Abstract

Computerized India is the aftereffect of numerous developments and innovative progressions. The greater part populace is in not in propensity for utilizing Computer, web and different gadgets which are most regularly utilized are online media locales (Facebook), visit rooms, skype, WhatsApp, Dating destinations and so forth. At one side of the coin the digitalization has upgraded the arrangement of India in all terms, for example, economy, training, administration and so forth, yet at second it brought cyber-crimes likewise in India everywhere number. The meaning of cybercrime keeps on advancing as roads open up that permit cybercriminals to target customers in new manners. Understanding the behaviour of cybercriminals and the engineering talents that are there within the field of cybersecurity among young people in India is essential in the current digital landscape. Because of the rapid increase in the number of people using the internet and the improvements in technology, young people are the primary consumers of digital platforms and also have the potential to be either the offenders or victims of malicious cyber activity. As a result, the investigation of their behaviours and capacities within the context of this situation is of tremendous importance. Young people in India engage in a wide variety of activities that fall under the category of cybercrime. These activities range from harmless inquiry and experimentation to unlawful hacking and fraudulent operations conducted online. The attitudes and behaviours that individuals exhibit in cyberspace are significantly influenced by a variety of factors, including their socioeconomic background, the influence of their peers, the availability of technology, and their exposure to cybersecurity education. Researchers are able to get insights into the motives, vulnerabilities, and risk factors that drive juvenile engagement in cybercrimes by delving into these dynamics and gaining a better understanding it.

Keywords: Cybercrime, Youth Behaviour, Act.**Introduction**

The Internet is one of the quickest developing spaces of specialized foundation development. Today, data and correspondence advances are ubiquitous and the pattern towards digitization is developing. The interest for Internet and PC network has prompted the reconciliation of PC innovation into items that have normally worked without it, like vehicles and buildings. Electricity supply, transportation framework, military administrations and coordinations - for all intents and purposes all advanced administrations rely upon the utilization of ICTs.

Cybercrime is any crime that includes a PC, organized gadget or an organization. While most cybercrimes are completed to create benefit for the cybercriminals, a few cybercrimes are done against PCs or gadgets straightforwardly to harm or incapacitate them, while others use PCs or organizations to spread malware, illicit data, pictures or different materials. A few cybercrimes do both - i.e., target PCs to contaminate them with a PC infection, which is then spread to different machines and, at times, whole organizations.

It is possible that doing research on the criminal behaviour of young people in India and evaluating their engineering capabilities in the field of cybersecurity could provide significant insights into the digital landscape of the respective country. For the purpose of designing successful strategies to combat cyber risks and promote digital safety, it is essential to have a solid understanding of how young people engage with cybercrime and their level of expertise in cybersecurity measures.

An essential impact of cybercrime is monetary; cybercrime can incorporate a wide range of sorts of benefit driven crime, including ransomware assaults, email and web extortion, and character misrepresentation, just as endeavors to take monetary record, Visa or other installment card data. Cybercriminals may likewise focus on a person's private data, just as corporate information for burglary and resale. As numerous laborers subside into far off work schedules because of the pandemic, cybercrimes are required to fill in recurrence in making it particularly essential to ensure reinforcement information. This partitions cybercrime into three classes:

*Research Scholar, Himalayan Garhwal University, Shiv Nagar, Phokra, India.

**Research Supervisor, Himalayan Garhwal University, Shiv Nagar, Phokra, India.

1. crimes in which the processing gadget is the objective - for instance, to acquire network access;
2. crimes in which the PC is utilized as a weapon - for instance, to dispatch a disavowal of-administration assault; and
3. crimes in which the PC is utilized as an assistant to a wrongdoing - for instance, utilizing a PC to store unlawfully got information.

Review of Literature

According to an article titled "Cyber Crime: A Threat to the Nation and its Awareness" by Monalisa Hati (2016) [2], India has been the target of numerous cybercrimes involving computers and the internet in the twenty-first century. The number of people utilising computers as well as the internet is increasing daily, and obtaining information is straightforward and expedient. Despite the implementation of stringent measures and diligent efforts, cybercrime, defined as unauthorised online activity, continues to escalate. I have discussed the damage that cybercrime causes to the nation, as well as preventative and awareness-raising measures that can be implemented to mitigate the risk, in this essay.

In her research titled "A Literature Review of Cyber Security," Pallavi Murghai Goel (2019) [4] found that the phrases cyber security and information protection are commonly used synonymously. This essay argues that while there are numerous parallels between cyber security and information protection, they do not totally line up. Furthermore, the paper argues that cyber security encompasses not just the protection of data but also other attributes, like the individual, and goes beyond the conventional notions of information security. The role(s) that people play in the information safeguarding process are usually brought up while discussing the human element. The potential for people to be the target with cyberattacks or perhaps unknowingly take part in them is another facet of cyber security. This extra element may be seen as a social duty to protect such disadvantaged groups, as children, which has ethical implications for society at large.

Moallem (2018) [5] This study presents preliminary findings from an investigation into student attitudes and awareness of cyber security & the associated hazards in the world's most technologically advanced region, Silicon Valley, California, USA. Learners in Silicon Valley come from a highly varied range of ethnic backgrounds. The aim of the study was to determine the level of awareness among students in this technologically advanced setting regarding cyber-attacks and their defence mechanisms. According to the preliminary

statistical research, college students are not well-informed on data protection, even though they think they are watched when they use the Internet as well as that their data is not safe even on university systems. Furthermore, it seems that academic institutions are not actively working to raise college students' awareness of these problems and teach them how to defend themselves against future cyberattacks like ransomware and identity theft.

Analysis

Cybercriminal movement might be completed by people or little gatherings with generally minimal specialized ability. Or then again, by profoundly coordinated worldwide criminal gatherings that may incorporate talented engineers and others with significant mastery. To additionally decrease the odds of discovery and indictment, cybercriminals frequently decide to work in nations with frail or nonexistent cybercrime laws. The following are some other factors to take into mind for your research on the engineering capabilities and cybercrime behaviour of young people in India:

1. Conduct A Demographic analysis to investigate the ways in which age, gender, education level, and socio-economic background influence the behaviour of Indian youth in relation to cybercrime and their ability to protect themselves from cyberattacks. It is possible to customise treatments to specific groups by first gaining an understanding of demographic patterns.
2. Motivations and Influences: Conduct research into the factors that motivate young people to participate in activities that involve cybercrime, as well as the factors that affect them to make decisions about whether or not to pursue careers in cybersecurity. An investigation into the sociological, cultural, and economic aspects that influence people's perspectives on digital security could be one way to do this.
3. Technological Landscape: Determine the current level of technological adoption and digital literacy among young people in India. This is the third step in the technological landscape. It is possible to offer context for their cybersecurity knowledge and behaviours by gaining an understanding of their expertise with a variety of digital platforms, devices, and applications.
4. Educational and Training Initiatives: Conduct an analysis of the efficacy of the existing cybersecurity education and training programmes that are aimed at young people in India. Determine the areas of the curriculum that are lacking in terms of coverage, instructional methods, and access to

resources that could potentially impede the development of cybersecurity abilities.

5. **Policy and Legal Frameworks:** Determine whether or not the rules and regulations in India that pertain to the prevention and prosecution of cybercrime are adequate. Evaluate the degree to which these frameworks cater to the ever-changing characteristics of cyber risks and determine whether or not they offer adequate deterrents for individuals who might commit cybercrime.

6. **Industry Engagement:** Explore the role that the private sector can play in cultivating cybersecurity talent among young people in India. This is the sixth step in the industry engagement process. Conduct research into the possibility of forming partnerships between educational institutions and industry stakeholders, as well as internship opportunities and initiatives that aim to encourage cybersecurity entrepreneurship.

7. **International Comparisons:** Consider comparing the findings of your study with those of similar studies undertaken in other countries in order to discover common difficulties and best practices in tackling criminal behaviour and boosting cybersecurity capabilities among young people.

Conclusion

It is of the utmost importance to incorporate engineering talents into cybersecurity education and training programmes for young people in India. This is necessary in order to cultivate a trained workforce that is capable of protecting digital assets and defending against cyber threats. In order to accomplish this, it is necessary for educational institutions, government agencies, industry partners, and cybersecurity specialists to work together in order to provide complete curricula, give opportunities for hands-on learning, and provide mentorship programmes. Through the cultivation of a generation of cyber defenders who are capable of securing the digital future of the nation, India can strengthen its cyber resilience and develop a generation of young people who are equipped with the essential knowledge, skills, and ethical values.

Cyber-crooks use PC innovation to get to individual data and use web for badgering and misuse purposes which incorporates following, extorting, undermining through messages, photograph transforming, cyber erotic entertainment and so on Presently a-days, culprits are progressively abusing Cyber stages to disturb and mishandle women and kids for voyeuristic delights in India. Women and youngsters are generally focused for cyber following, provocation, coercion, extortion, and so forth The Women

frequently trust culprits or victimizer and offer their own data which results various cybercrimes. Commonly, culprits get an opportunity to disturb, misuse, shakedown and so forth the lady and youngsters more since they are ignorant about the methodology of documenting an objection. Huge mindfulness should be made among women and youngsters with respect to the sheltered utilization of Mobile Phones, Computers and the Internet. At the same time, it is critically important to evaluate the technical capabilities of young people in India in the field of cybersecurity in order to construct strong defences against cyber threats. The evaluation of their technical skills, awareness of cybersecurity concepts and practices, competency in programming languages and tools, and aptitude for problem-solving in the digital environment are all components of this process. A better awareness of the competences that stakeholders possess in areas such as network security, cryptography, ethical hacking, and malware analysis allows them to identify areas of strength that may be leveraged and areas in which they can improve their skills.

Conflict of Interest

There is no conflict of interest by the authors in this manuscript.

References

1. Taha, N. and Dahabiyeh, L. (2020). College students information security awareness: A comparison between smartphones and computers. *Educ. Inf. Technol.*, 26, 1-16.
2. Hati, Monalisa (2016). Cyber Crime: A Threat to the Nation and its Awareness. *International Journal of Advanced Research in Computer and Communication Engineering*, 5(7), 690- 692.
3. Wash, Rick and Cooper, Molly M. (2018). Who Provides Phishing Training?: Facts, Stories, and People Like Me. In *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI '18)*, ACM, New York, USA.
4. Goel, Pallavi Murghai (2019). A Literature Review of Cyber Security. *International Journal of Research and Analytical Reviews (IJRAR)*, 6(2), 136-141.
5. Moallem, A. (2018). Cyber Security Awareness Among College Students. In *International Conference on Applied Human Factors and Ergonomics*, Springer: Berlin/Heidelberg, Germany, 79-87.