# Realities and Challenges of Cybercrimes in India: An Analytical Study

**POOJA BAHUGUNA**
Assistant Professor,Department of Faculty of Law , Graphic Era Hill University, Dehradun Uttarakhand India 248002 ,

## Abstract

This investigative scrutiny delves into the veracity and complexities of digital wrongdoings in India. The nation has witnessed a momentous surge in the quantity of digital wrongdoings in the recent period, prompting financial predicaments and disrepute in personal eminence. The analysis scrutinizes the various categories of digital wrongdoings that prevail in India, encompassing the malevolent activities of hacking, pilfering of personal identities, deceiving ploys of phishing and the vicious assaults of ransomware. Additionally, it evaluates the elements that foster the escalation of digital wrongdoings, such as the rapid and widespread proliferation of technology, inadequate discernment among the populace and the insufficiency of robust measures in cybersecurity. The study further discusses the legal framework and institutional mechanisms in place to combat cybercrimes in India, including the Information Technology Act, 2000, and the National Cyber Security Policy, 2013.The current discourse highlights the obstacles faced by authorities in their pursuit of cybercriminals. This is primarily due to the intricate nature of cybercrimes. The study puts forth the necessity for a comprehensive approach in addressing cybercrimes in India. This would entail a combination of legal, technological, and educational measures aimed at raising public awareness and fortifying cybersecurity infrastructure.

Keyword: Cybercrimes, Cybersecurity, Legal and Technological Education, Investigative Scrutiny, Realities and Challenges

## Introduction

India has made remarkable strides in the sphere of technology and is now setting its sights on evolving into an information society through its grandiose "Digital India" endeavor. The conceptual foundation behind this scheme is to exploit digital technologies to actualize a lucid, proficient, and easily reachable government, whilst enabling the private sector and individuals to utilize the internet to transact sensitive dealings and hoard pivotal data on the cloud. Notwithstanding the potential of this initiative to metamorphose the country, it also lays India open to the perils of cybercrimes.

According to Das and Nayak (2013) the increasing adoption of digital technologies has led to a rise in cybercrimes in India. Cybercrimes refer to criminal activities that are committed using the internet or any other form of digital communication. These crimes can take many forms, including hacking, identity theft, phishing, ransomware attacks, and more. These cybercrimes have resulted in financial losses and damage to personal reputation, which can have long-lasting consequences. India's susceptibility to cybercrimes can be attributed to a multitude of factors, including the expeditious proliferation of technology, the general populace's paucity of cognizance, and deficient cybersecurity protocols. Owing to the ubiquitous adoption of digital technologies, India has become increasingly reliant on the internet, rendering it a prime target for cyber malefactors. Furthermore, numerous denizens of India are not cognizant of the risks attendant upon internet usage, such as phishing attacks and other fraudulent schemes.

Narahari and Shah (2016) conducted a study and found this dearth of cognizance renders them susceptible to cyber incursions. Moreover, India's cybersecurity infrastructure needs significant improvement to counter cybercrimes. While the government has enacted laws to combat cybercrimes, such as the Information Technology Act, 2000, and the National Cyber Security Policy, 2013, these measures are not enough to tackle the scale and complexity of cybercrimes. Additionally, the lack of skilled personnel and inadequate resources hampers the effective implementation of these laws.Investigating and prosecuting cyber offenses pose significant challenges due to the intricate nature of these crimes. Cybercriminals can effortlessly conceal their identity and location, making it arduous for law enforcement agencies to locate and track them. Moreover, the global scope of cyber offenses adds another layer of complexity, as perpetrators can operate from any part of the world, rendering them unaccountable. To surmount these challenges, India necessitates a comprehensive approach to combat cyber offenses, encompassing a combination of legal, technological, and educational measures. The government must invest in cybersecurity infrastructure and personnel to counter cyber offenses efficaciously. It is essential to analyse the realities and challenges of cybercrimes in India to understand the extent of the problem and develop effective strategies to combat it. This analytical study aims to explore the current state of cybercrimes in India, the types of cybercrimes prevalent in the country, their impact on individuals and organizations, and the challenges faced by law enforcement agencies in combating these crimes. By providing a comprehensive analysis of the realities and challenges of cybercrimes in India, this study hopes to raise awareness and facilitate the development of effective policies and strategies to combat this growing threat. Figure 1 shows the various reasons of cybercrimes in India.

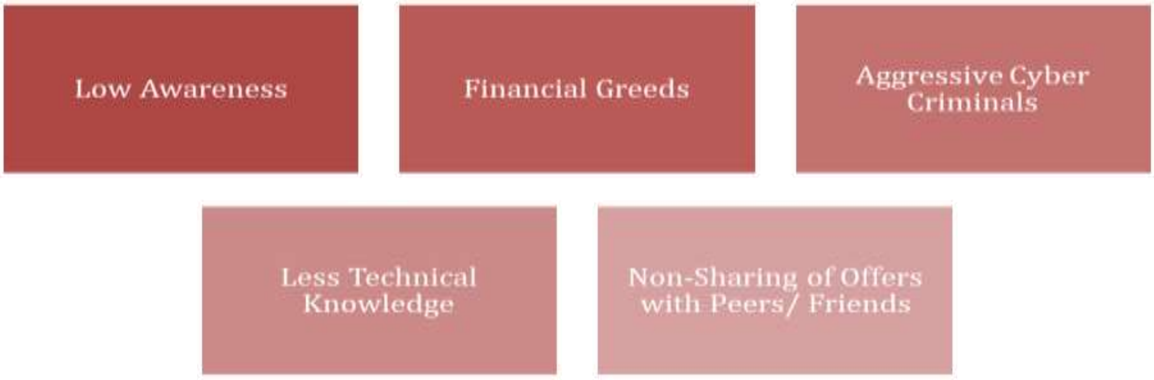
Low Awareness
Financial Greeds
Aggressive Cyber Criminals
Less Technical Knowledge
Non-Sharing of Offers with Peers/ Friends

**Figure 1 Reasons of Cybercrimes in India**

## Literature Review

India has emerged as a rapidly growing economy in the global landscape, with an expanding digital economy that has brought with it the unfortunate side effect of increased cybercrime. Cybercrime is the criminal use of computers or the internet, and it poses a serious threat to India's digital economy. Shah (2016) conducted a study and found the issue is multifaceted, and it demands a comprehensive understanding of the various realities and challenges that must be overcome to effectively address it. The National Crime Records Bureau (NCRB) reported a sharp rise in cybercrime incidents in India, increasing by 63.5% between 2017 and 2018. This concerning trend highlights the urgent need for prompt action to combat this issue. The gamut of cyber offenses pervasive in India is wide-ranging, encompassing hacking, phishing, cyberstalking, identity theft, cyberbullying, and online financial frauds, inter alia. These illegal activities are perpetrated by cyber malefactors who employ intricate techniques to target individuals, businesses, and organizations.

Dhar (n.d.) critically evaluated and revealed in recent times, India has been encountering an upsurge in cybercrime episodes of various sorts, ranging from hacking, phishing, cyberstalking, identity theft, cyberbullying, and online financial frauds, among other forms of cyber malfeasance. Hacking, a type of cybercrime that involves unauthorized access to computer networks or systems, has been on the rise in India with many prominent cases reported in recent times. The objectives behind these hacking incidents can vary from political activism to the desire for monetary gains. Phishing, a nefarious form of cybercrime, runs rampant in the country of India. This type of digital deception entails dispatching counterfeit emails or messages that are made to look like they originate from genuine sources, all with the intention of ensnaring the recipient into divulging their private information, including, but not limited to, login credentials or financial particulars. The intricacy of these phishing scams has increased considerably over time, rendering it a Herculean task for people to discern between veritable and counterfeit communiqués. In the realm of digital communication, cyberstalking, a malevolent act that leverages the power of technology to instil fear or harass an individual, is a menacing phenomenon. The ubiquitous social media platforms provide a convenient tool for perpetrators to execute their nefarious deeds.

Kshetri (2016) discussed and found the deleterious impact of cyberstalking on the psychological and physical well-being of a person is a matter of great concern. India, too, has been grappling with the menace of cyberstalking, particularly targeted against women. Identity theft, a form of cybercrime that entails the misappropriation of personal information for fraudulent purposes, is a grave threat to individuals. The ramifications of this pernicious crime extend beyond the financial domain, leaving an indelible blemish on one's reputation. In India, the banking and financial sectors have witnessed instances of identity theft, posing a severe threat to the victims' financial health and stability. With the advent of technology, individuals have increasingly resorted to utilizing social media platforms to perpetuate harassment, intimidation, or humiliation, commonly referred to as cyberbullying. This malevolent behavior has grave psychological consequences and, in severe cases, may even result in the victim resorting to suicide. In India, the pervasiveness of cyberbullying has become a growing concern, particularly among children and teenagers. Additionally, online financial fraud is a significant threat to India's digital economy, with cybercriminals employing technology to conduct fraudulent financial transactions such as the illicit acquisition of credit card information or the unauthorized transfer of funds from bank accounts.

Nayak and Panda (2015) revealed that the repercussions of online financial fraud can be disastrous, with victims incurring financial losses and reputational harm. However, despite the exponential rise in cybercrime incidents in India, the conviction rate in such cases remains astoundingly low. While several factors contribute to this, the current scenario undeniably poses a significant challenge for law enforcement agencies. Primary reasons behind the low conviction rate are the dearth of competent professionals who can handle such cases. Cybercrimes necessitate specialized skills and knowledge to investigate and prosecute, which are presently inadequate in India. Moreover, the current legal framework fails to extend adequate support to law enforcement agencies during cybercrime investigations, which ultimately results in poor conviction rates. Another significant factor is the insufficiency of an appropriate cybersecurity infrastructure.

Rao and Ramya (2018) found that India’s cybersecurity infrastructure is relatively underdeveloped, rendering it easier for cybercriminals to operate with impunity. Furthermore, insufficient infrastructure implies that law enforcement agencies lack the required capabilities to deal with the sophisticated techniques utilized by cybercriminals. The intricacy of cybercrime cases is yet another contributing factor to the low conviction rate. Cybercrimes frequently entail multiple jurisdictions, making it arduous for law enforcement agencies to collaborate effectively. Additionally, the technical expertise demanded to handle cybercrime cases renders it challenging for law enforcement agencies to amass evidence and construct a sturdy case. The occurrence of cybercrime cases that go unreported is rampant due to the dread of social ostracism or the conviction that reporting will not result in legal retribution. The feeble awareness of the populace concerning the significance of notifying incidents of cybercrime is likewise a contributing factor to the dismal conviction rate. Raising the consciousness of people about the necessity to notify such occurrences and instilling confidence in the justice system to dispense impartial judgments is paramount.

Reddy (2014) examined and revealed that the Indian government needs to devote resources to building a robust cybersecurity infrastructure to confront the challenge of low conviction rates. This includes augmenting the number of adept professionals trained in investigating cybercrime, devising a specialized department for cybercrime investigation, and establishing courts that handle cybercrime cases exclusively. It is imperative to raise awareness amongst the general populace about the importance of cybersecurity and promptly reporting incidents of cybercrime. This would serve to greatly reduce the incidence of cybercrime and enhance conviction rates. Despite the escalating numbers of cybercrime occurrences, many individuals remain oblivious to the risks and measures they can take to safeguard themselves against online threats. One of the most frequent ways through which cybercriminals capitalize on this lack of awareness is via phishing scams.

Gangadharan (2018) discussed and revealed Phishing is a deceitful ploy employed by cybercriminals to deceive people into divulging their private information, including bank account details, credit card numbers, and passwords. The fraudsters utilize various stratagems to convince the victim that they are trustworthy and legitimate, such as creating spurious websites or dispatching counterfeit emails. Many individuals still fall prey to fraudulent activities due to a lack of knowledge about cybersecurity measures. These individuals are unaware of the severe consequences that may arise as a result of revealing confidential information, such as financial losses, identity theft, and reputational harm. To mitigate this problem, it is imperative to increase awareness of cybersecurity measures among the general public. Educational endeavors must be undertaken to provide people with knowledge about the hazards of cybercrime and the measures they should take to protect themselves. One approach to accomplishing this goal is to launch public awareness campaigns.

Jain (2017) examined and found the government could collaborate with private organizations and cybersecurity experts to conduct campaigns aimed at educating the public about the risks of cybercrime and the precautions they should take. Such campaigns could be disseminated through various mediums, including television, radio, social media, and other online platforms. Additionally, schools and universities represent another viable method of increasing awareness. Cybersecurity should be included in the curriculum, and students should be educated about the risks and measures they should take while using the internet. This approach could create a cybersecurity-aware culture among the younger generation.Moreover, it is crucial for organizations to play a pivotal role in promoting cybersecurity awareness. Regular training sessions should be conducted to educate employees about cybersecurity measures and the risks of cybercrime. This will help create a cybersecurity-conscious workforce and reduce the likelihood of data breaches and other cyber incidents. However, underreporting cybercrimes remains a significant challenge in India, despite an increase in cybercrime incidents. Numerous cases go unreported due to reasons such as a lack of awareness, fear of retaliation, and mistrust in law enforcement agencies.

Underreporting is primarily due to a lack of awareness among the public about cybercrime and its implications. People may not know how to report cybercrime incidents or might not be aware that they were victims of such a crime. Ignoring or handling incidents by themselves often leads to more severe outcomes. Another reason is the fear of retaliation by the cybercriminals. They can easily identify and target victims, which can lead to further harassment or retaliation. This fear of retaliation can further increase underreporting of cybercrime incidents. Additionally, a lack of trust in law enforcement agencies exacerbates the problem of underreporting. People are not confident that the agencies will handle their complaints effectively. There is often a fear that their complaints will be ignored or mishandled, which causes a lack of trust in the system. Creating awareness about cybercrime reporting procedures among the public is crucial to address underreporting. The government and private organizations should collaborate to launch public awareness campaigns that educate people about the importance of reporting cybercrime incidents and the procedures for doing so. Improving the trust and confidence of the public in law enforcement agencies is also necessary. These agencies should be adequately equipped and trained to handle cybercrime incidents effectively. They should work towards building trust among the public by being responsive and transparent in their handling of cybercrime cases.

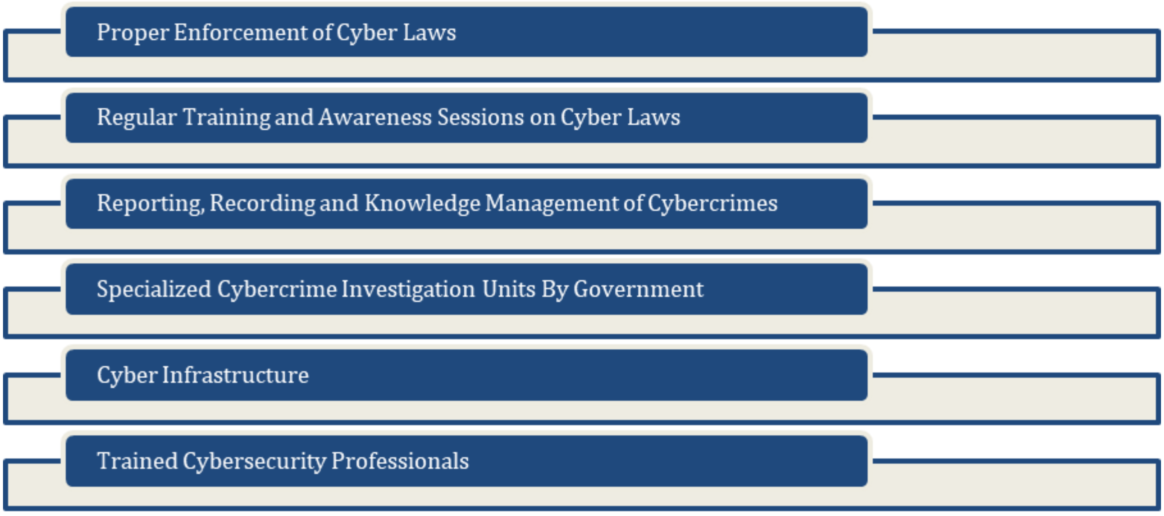
Proper Enforcement of Cyber Laws
Regular Training and Awareness Sessions on Cyber Laws
Reporting, Recording and Knowledge Management of Cybercrimes
Specialized Cybercrime Investigation Units By Government
Cyber Infrastructure
Trained Cybersecurity Professionals

**Figure 2 Solutions of Cybercrime**

Strengthening the legal framework for cybercrime is also crucial. The government should enact stricter laws to deter cybercriminals and ensure that the victims receive justice. Moreover, the government should establish specialized cybercrime investigation units to handle cybercrime cases effectively. Unfortunately, the infrastructure for cybercrime investigation in India is still underdeveloped, and there is a lack of trained personnel to investigate cybercrimes effectively. This has resulted in low conviction rates and a lack of justice for the victims. Based on the review of extant literature, figure 2 has been prepared which offers the solutions of cybercrimes.

India's fight against cybercrime is the lack of infrastructure for cybercrime investigation. The country still lacks adequate tools and technology to investigate and prosecute cybercrimes effectively. Moreover, existing laws and regulations are often outdated and do not cover the rapidly evolving nature of cybercrime. This lack of infrastructure and technology has made it difficult for law enforcement agencies to track and apprehend cybercriminals. Another challenge is the shortage of trained personnel to investigate cybercrimes. Cybercrime investigation requires specialized skills and knowledge, which many law enforcement agencies lack. Furthermore, the training and education programs for cybercrime investigation are still inadequate in India. This shortage of trained personnel has led to a backlog of cases, delayed investigations, and low conviction rates. To address these challenges, the Indian government has taken several initiatives to strengthen the cybercrime infrastructure. The government has established cybercrime investigation units in various parts of the country and is investing in the latest technology and tools to investigate cybercrimes. Additionally, the government is also collaborating with private organizations and international agencies to build a robust legal framework to combat cybercrime.

## Conclusion

The issue of cybercrime is a growing concern in India. The rapid growth of technology has brought about new challenges and realities for law enforcement agencies and the government. The increasing number of cyberattacks and their sophisticated nature have made it difficult for authorities to combat these crimes effectively. The lack of awareness among the general public about cyber threats and the absence of strict cyber laws have only exacerbated the problem. The study has shed light on the various types of cybercrimes prevalent in India, including hacking, phishing, identity theft, and cyberbullying. It has also highlighted the challenges faced by law enforcement agencies, such as the lack of trained personnel and the need for better technology and infrastructure. The study suggests that there is a need for greater collaboration between the government, law enforcement agencies, and the private sector to combat cybercrime effectively. It recommends the implementation of strict cyber laws, capacity building programs for law enforcement agencies, and awareness campaigns for the general public.

### References

1. Das, S., & Nayak, T. (2013). Impact of cybercrime: Issues and challenges. *International journal of engineering sciences & Emerging technologies*, *6*(2), 142-153.
2. Narahari, A. C., & Shah, V. (2016). Cyber Crime and Security–A Study on Awareness among Young Netizens of Anand, Gujarat State, India. *IJARIIE*, *6*(2), 1164-1172.
3. Shah, J. (2016). A study of awareness about cyber laws for Indian youth.
4. Dhar, M. P. Changing Dimensions Of Criminal Jurisprudence In Virtual Reality": A Critical Evaluation Of Information Technology Laws,' Cyber Crimes And Crimes Per Se'in India.
5. Kshetri, N. (2016). Cybercrime and cybersecurity in India: causes, consequences and implications for the future. *Crime, Law and Social Change*, *66*, 313-338.
6. Nayak, S. K., & Panda, C. S. (2015). A Study of Cyber Security Issues and Challenges on Latest Technologies in India. *International Journal of Management, IT and Engineering*, *5*(11), 136-146.
7. Rao, A., & Ramya, U. (2018). Globalism: Challenges & Opportunities For Better Tomorrow Theme: Understanding Of Digital Age. *Department of Commerce Bangalore University*, 103.
8. Reddy, K. S. (2014). Cyber Crimes in India and the Mechanism to Prevent them.

9. Gangadharan, V. N. (2018). Need for Police Reforms in India Police Reforms vis-a-vis Cyber Crimes. *Available at SSRN 3835257*.
10. Jain, M. (2017). Victimisation of women beneath cyberspace in Indian upbringing. *Bharati Law Review*, *4*.
11. Dosi, R., & Khanna, P. (2012). E-Jurisprudence In The Indian Criminal System: Challenging Cyber Crimes In Every Aspect. *Law Technology*, *45*(1), 1.
12. Thapa, A., & Kumar, R. (2011). Cyber stalking: crime and challenge at the cyber space. *An International Journal of Engineering Sciences*, *4*, 340-354.