ISSN: 2583-6285 ***Volume 3, Issue 2; April 2024***

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYSIS IN COMMERCE AND MANAGEMENT

Web: https://www.iarj.in/index.php/ijracm/issue/archive

1. A Study on Cyber Fraud Threating Digital India User

Dr. Roy Anita Kumari Parmanand
Assistant professor, Dept. of Commerce,
Marwari College,
Darbhanga, Bihar.

ABSTRACT

India has seen a notable increase in cybercrime cases in recent years. Cybercrime has become more common as digital technology has become more and more integrated into our daily lives. The causes of the surge in cybercrime in India, its wide-ranging effects, and the crucial safety precautions people and businesses can take to keep themselves safe are all covered in this article. In today's world, it is inconceivable to imagine life without the internet.

Every day, billions of individuals connect over the internet. Daily chores including banking, R&D, communication, travel, and education are all facilitated by the internet. India is among the many nations that are undergoing digitalization for development purposes, but there are drawbacks as well. As the nation embraces programs like "Digital India," the likelihood of cybercrime is increasing. There are pros and cons to technology adoption in a variety of industries. The Internet of Things (IOT) is encompassing everything from power grids to finance and agriculture. Numerous security issues are linked to the progress of digitalization and require immediate response. This paper will talk about. A Study on Cyber Fraud Endangering Users of Digital India.

KEYWORDS

Cyber Fraud, Threating, Digital India, Cybercrime, Internet, Mobile Devices, Economic Incentives, Malware, SQL Injection, Phishing.

Introduction:

Cybercriminals are extremely knowledgeable about police and enforcement agency procedures, and their ability to replicate real-looking offices, clone websites of regulatory agencies and courts, and spoof social media handles is enough to scare people these days, especially in light of the frequent reports in the media about how police from one state can arrest someone in another, arrange for transportation, and imprison them in a place where they have no family, support system, or other resources. [1]

"Any unlawful act where computer or communication device or computer network is used to commit or facilitate the commission of crime" is the general definition of cybercrime. Globally, the frequency of cybercrimes is increasing at an exponential rate, leading to significant financial and personal losses. According to data provided by the National Crime Records Bureau (NCRB) in its publications, the number of cybercrimes reported in India increased by 143 percent in just five years, from 21796 in 2017 to 52974 in 2021. This study's goals are to analyze data on cybercrime in India from 2017 to 2021, comprehend the reasons behind these crimes, and outline the steps the government has made to prevent them. There will also be a discussion on precautions people can take to shield themselves against cybercriminals. [2]

The Factors Driving the Rise of Cybercrime in India

Rapid Digitization: Millions of Indians now have internet access because to the country's quick digitization efforts, which include programs like Digital India. Although there are many advantages to this, a greater population is now vulnerable to cyber threats. In order to secure themselves, a lot of people and organizations might not have the required cybersecurity infrastructure and awareness.

Inadequate Cybersecurity Awareness: A considerable segment of the Indian populace lacks sufficient knowledge regarding online risks and optimal methods for ensuring digital security. People who are unaware of this are more susceptible to internet fraud, phishing attacks, and other cybercrimes.

Increasing Use of Mobile Devices: Cybercriminals now find it simpler to target specific people with mobile-based assaults due to the widespread use of smartphones and the expansion of mobile internet. Users of mobile devices might not be as careful as they should be because of their ease.

Economic Incentives: An increasing number of criminals have been drawn to cybercrime due to the accompanying cash rewards. The possibility of financial gain drives cybercriminals to carry out ransomware attacks on organizations as well as break into personal bank accounts.

Cybercrime Trends in India

Approximately 5,000 cyber complaints are sent to the Indian Cyber Crime Coordination Centre (I4C) every day, with roughly half coming from overseas. Sextortion, fraudulent apps linked to investments, fraudulent loan apps, impersonation on social media, and customer care scams are some of the main themes that have been noticed. The largest instances are reported in union territories like Delhi, Chandigarh, and Puducherry and states like Haryana, Telangana, Uttarakhand, Gujarat, and Goa.

Impact of Cyber Crimes

- Multifaceted threats are posed by cybercrimes.
- National Security: They have the ability to undermine government and vital infrastructure.

- Financial Loss: This might include ransomware attacks and fraud involving online banks.
- Data breaches: Resulting in the disclosure of private and confidential company data.
- Disruption of Services: Impacting vital services such as electricity and communication networks.
- Reputational damage: When an organization's brand and consumer base are damaged.
- Rising Cybersecurity Costs: Businesses are facing higher operating costs.

National Cyber Security Policy:

The Department of Electronics and Information Technology has developed the National Cyber Security Policy as a foundation for policy. Its goal is to defend against cyberattacks on both public and private infrastructures. Additionally, "information, such as personal information (of web users), financial and banking information, and sovereign data" is what the policy aims to protect. With no technological or legal protections against it, Indian consumers are allegedly being spied on by US government agencies, which made this more pertinent in the wake of NSA exposures. Cyberspace is defined by the Indian Ministry of Communications and Information technologies as a complex environment made up of human interactions and software services facilitated by the global dissemination of information and communication technologies.

Vision

To prevent anyone from invading a user's privacy and to create a robust and safe cyberspace for organizations, governments, and citizens.

Mission

Building capacities to prevent and respond to cyber threats, reducing vulnerabilities and minimizing damage from cyber incidents through a combination of institutional structures, people, procedures, technology, and cooperation are all necessary to secure information and information infrastructure in cyberspace. [4]

Types of Cyber Threats

Three types of threats are addressed by cyber-security:

1. Cybercrime includes both individual and group targets who aim to disrupt or gain from systems.
2. Information gathering for political purposes is frequently a part of cyberattacks.
3. The goal of cyberterrorism is to compromise electronic systems in order to incite fear or panic.

Some typical techniques to jeopardize cyber-security include the following:

- **Malware:** Software that is malicious is referred to as malware. Malware, which is designed by hackers or cybercriminals to cause disruptions or harm to legitimate users' computers, is one of the most prevalent cyberthreats. Malware can be utilized by

cybercriminals for financial gain or in politically motivated cyberattacks; it is typically distributed through unsolicited attachments in emails or downloads that look legitimate.

- **SQL injection:** A sort of cyberattack called a SQL (structured language query) injection is used to gain access to databases and steal data from them. Cybercriminals use vulnerabilities in data-driven applications to send malicious SQL statements into databases, inserting malicious code. They can now access the sensitive data kept in the database as a result.
- **Phishing:** Phishing is the practice of cybercriminals requesting sensitive information from victims via emails that seem to be from a reputable company. Phishing attacks are frequently used to trick people into divulging personal information, including credit card numbers. [5]

The Dangers of Cyber Fraud:

There is a rise in cyber fraud. The deadliest cyber fraud assaults, such as ransomware, spear-phishing, and business email infiltration, all start with an email. Because humans are the weakest link in your organization, email scams consistently work. One careless user can enable a cyber-fraud attack even with all your technological and human resources to prevent scam emails.

Cyber fraud can have catastrophic consequences. Theft of sensitive material, such as personally identifiable information and customer lists, can result in fines and legal issues. An employee may be tricked into sending substantial amounts of money to a bogus account by a phony email from the CEO. In addition, a company may lose customers, revenue, and money as a result of ransomware and other cyberfraud assaults disrupting operations.

Technology, training, and experience must all be combined in a multifaceted strategy to combat cyber fraud. For solutions to thwart email-borne threats, businesses all over the world turn to Mimecast.

Review of Literature:

All things considered, the internet, computers, and different mobile technologies have completely changed the way we live. Our interactions with and perceptions of the world around us have changed as a result of the widespread use of digital technology and the convergence of computing and communication devices. For shopping, entertainment, communication, banking, and information sharing, the physical world has given way to the digital one (Holt, 2016). [6]

These advancements are a double-edged sword, regardless of their overwhelming good effects. Without a doubt, every development also makes a space that can be used for illegal activity, supporting the adage that "crime follows opportunity." Our increasing reliance on computers and digital networks makes the technology itself an alluring target, either for information theft or as a means of causing disruption and damage. Examples include the misuse of photos shared online by child pornographers, online banking fraud, ATM fraud, stalking and harassment through email and SMS, and copyright infringement due to the ease of sharing digital media (Clough, 2010). [7]

Crimes against authority, such as cyberterrorism and attacks on satellites and electrical grids, are included in the category of cybercrime. Criminal activity directed towards individuals, including cyberstalking, defamation, and harassment. Phishing and virus injection into devices are examples of crimes against assets.

Data breaches are more likely since security organizations and states must store and transport large volumes of data across the Internet. Such significant hazards endanger the security of the country. India needs to maintain its cybersecurity because it is becoming a major hub for global IT.

To that end, the government of India has started a program dubbed "Digital India," which focuses on a number of important areas including banking, the health sector, digital literacy, safe and secure cyberspace, and many more. India has seen significant change in a short amount of time, yet the nation's growing Digital India is also seriously threatened by cyber security. (Kesharwani, 2019) [8]

Objectives:

- To understand various types of cyber-attacks and cyber-crimes
- To learn threats and risks within context of the cyber security
- To understand the Cyber Security Techniques which can be used stop such malicious activities from rising.

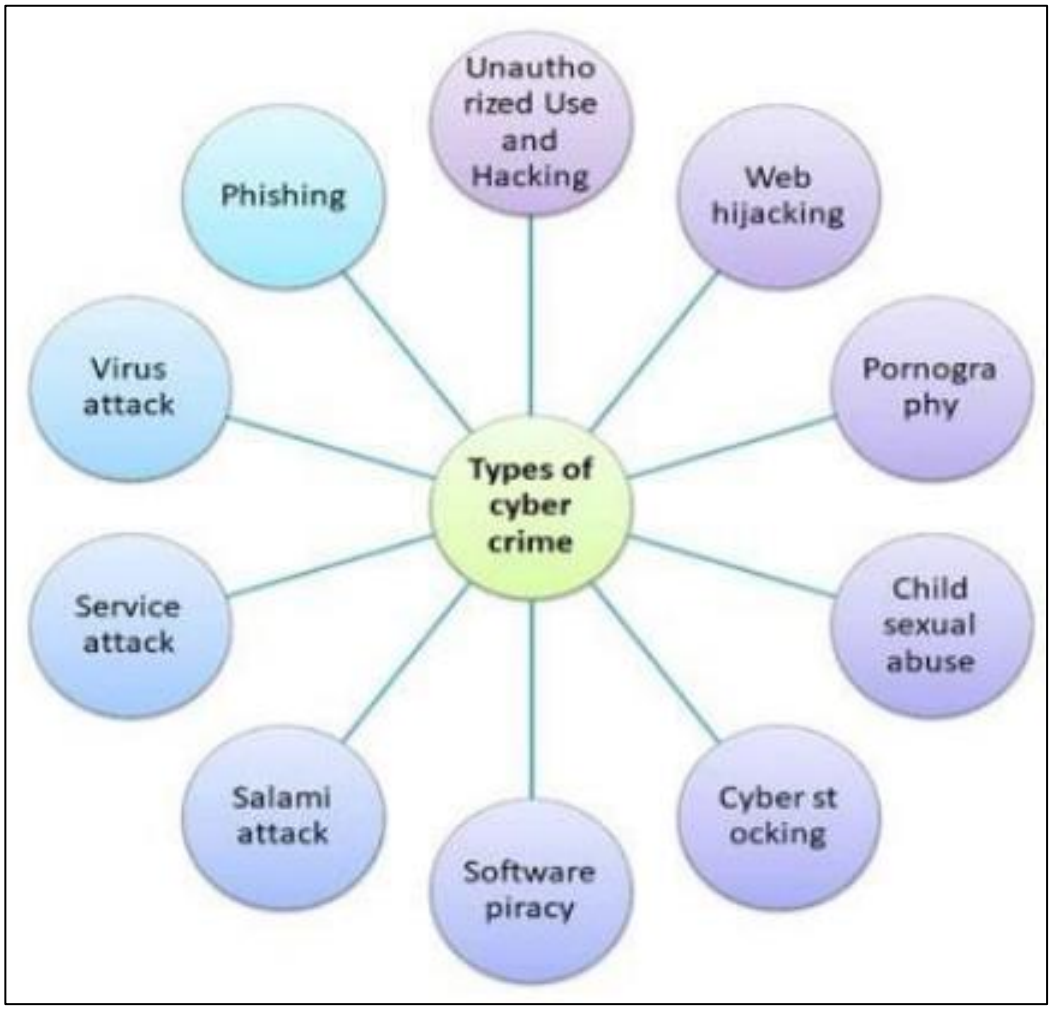
Research Methodology:

The overall design of this study was exploratory. The research paper is an effort that is based on secondary data that was gathered from credible publications, the internet, articles, textbooks, and newspapers. The study's research design is primarily descriptive in nature.

Result and Discussion:

Cyber-Crime:

The Internet is among the most significant inventions of the twenty-first century. These days, the internet has taken away all obstacles and transformed how we communicate, play games, work, shop, meet new people, watch movies, place food orders, pay bills, and celebrate life's milestones with loved ones. Given the increase in cyberattacks and threats, cybersecurity is the most important issue. Sophisticated techniques are being used by fraudsters to target the systems. All parties are impacted: individuals, small and large companies. All firms, IT and non-IT, have therefore come to understand the importance of cyber security and are making every effort to establish all available defenses. In some definitions, cybercrime is thoroughly explained. According to the Oxford Dictionary, cybercrime refers to "criminal activities conducted using computers or the Internet." "Cybercrime may be said to be those species, of which a genus is a conventional crime, and where either a computer is an object or subject of the conduct constituting crime," according to the definition of the word. A few of the many methods available for committing cybercrimes are listed in Figure (1) below. [9]



Analysis of Cybercrimes in India:

With more than 560 million internet users, India is the second-largest online market in the world, trailing only China. Additionally, it is predicted that the nation would have over 650 million internet users by 2023.

In India, 27, 248 incidences of cybercrime were reported in 2018, according to data from the National Crime Records Bureau (NCRB).

In Telangana, 1205 incidences of cybercrime were reported in one year. India ranks third among the top 20 countries affected by cybercrime, per an FBI assessment. Since its launch by the federal government last year, the national cybercrime reporting portal (cybercrime.gov.in) has received 33,152 complaints, leading to the filing of 790 FIRs.

As to a 2017 research, cybercrimes have caused Indian consumers to lose more than 18 billion US dollars. In 2018, the number of cybercrimes reported in the nation increased to over 27,000, a 121% rise over the same period the previous year. [10]

Table 1: Total number of cybercrimes reported in India from 2012-2018

Number of cybercrimes:

2018	27,248
2017	21,796
2016	12,317
2015	11,592
2014	9,622
2013	5,693
2012	3,377

The preceding table unequivocally demonstrates India's rising cybercrime case count. The top 5 most common cybercrimes are identity theft, cyberstalking, online harassment, phishing scams, and invasions of privacy.

Due to the COVID-19 epidemic and the lockdown, more people are confined to their homes, spending a greater amount of time online every day, and depending more and more on the Internet to acquire things they would typically only be able to obtain offline.

Although there have always been risks associated with cybercrime, the growing number of people who are online and the amount of time they spend there, along with the feeling of isolation and the anxiety and fear that come with a lockdown, have made it easier for cybercriminals to take advantage of the situation and increase their profits or cause disruption.

It is noteworthy that certain more susceptible groups of people, including kids, require greater internet time for things like education. E-crimes are on the rise as a result of this profound shift in how we use the Internet and conduct our lives. Phishing is one of the more popular cybercrime strategies. Phishing is the fraudulent activity of using fake websites or emails to trick people into disclosing personal information, including credit card numbers and passwords. [11]

According to the research, India ranks 11th globally in terms of the quantity of attacks that are generated by servers located there; 2,299,682 events were reported in Q1 2020, compared to 854,782 incidents in Q4 2019.

Data from the National Commission for Women (NCW) show that there were 54 online cybercrime complaints in April compared to 37 online and postal complaints in March and 21 complaints in February. As a result of the lockout, the panel is accepting online complaints. There were 412 valid reports of cyber abuse from March 25 to April 25, but cyber specialists claimed that these figures are only the "tip of the iceberg." 396 of these complaints, including abuses, indecent exposures, unsolicited pornographic photographs, threats, fraudulent emails saying their account was hacked, ransom demands, extortion, and more were from women.

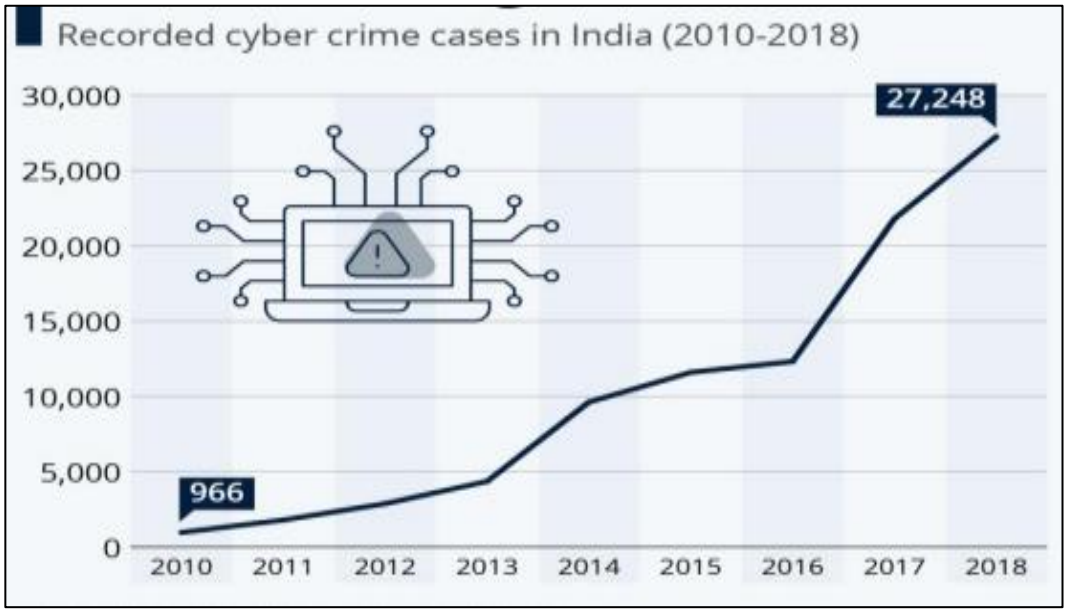


Figure 1: Sharp Increase of Cyber Crime in India during last decade (Source: - www.Statista.com visited on- 25 Nov 2020, 10:20)

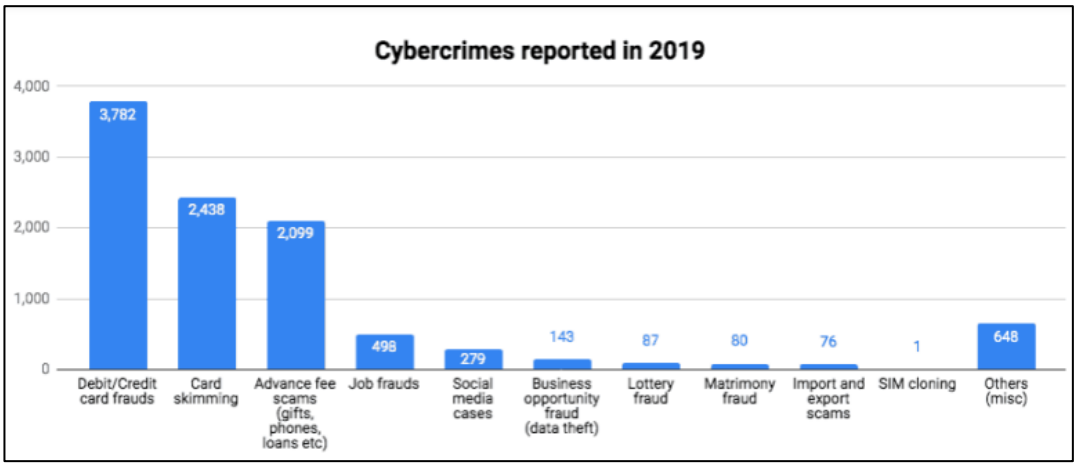


Figure 2: Cybercrimes reported in 2019 (Source: - www.Statista.com visited on- 25 Nov 2020, 08:20) [12]

Most number of Cyber Crimes reported in Maharashtra & Uttar Pradesh:

The rise in cybercrimes has coincided with the country's rising use of mobile and internet technologies.

Over 32,000 cybercrimes were detected nationwide between 2011 and 2015. Of these, over 24,000 are registered under the IT Act, with the rest instances falling under different IPC provisions and other State Level Legislations (SLL).

There has been a steady increase in the quantity of cases filed under the IT Act and IPC. From 2011 to2015, the number of cases filed under the IT Act increased by about 350%. Between 2013 and 2014, there was a nearly 70% rise in cybercrimes covered by the IT Act. In the years between 2011 and 2015, the number of IPC cases registered over 7 times.

The number of people arrested shows a similar pattern. The government admits that there have been more of these crimes, and that this spike in crime is a direct result of the introduction of new technology, gadgets like smart phones and sophisticated programs, and an increase in the use of the internet by businesses. [13]

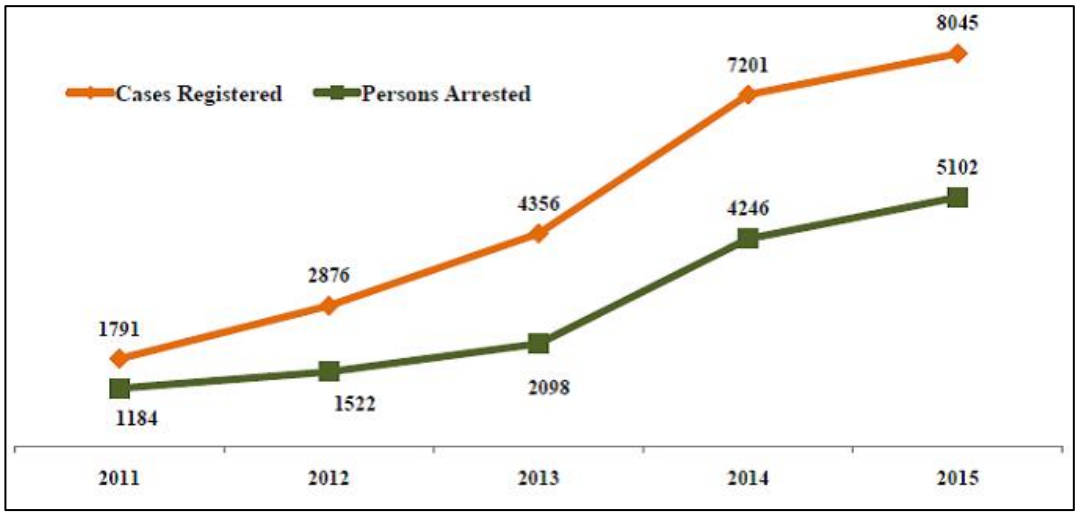


Figure 3: Cyber Crime in India- Cases Registered Under IT Act (2011-15)

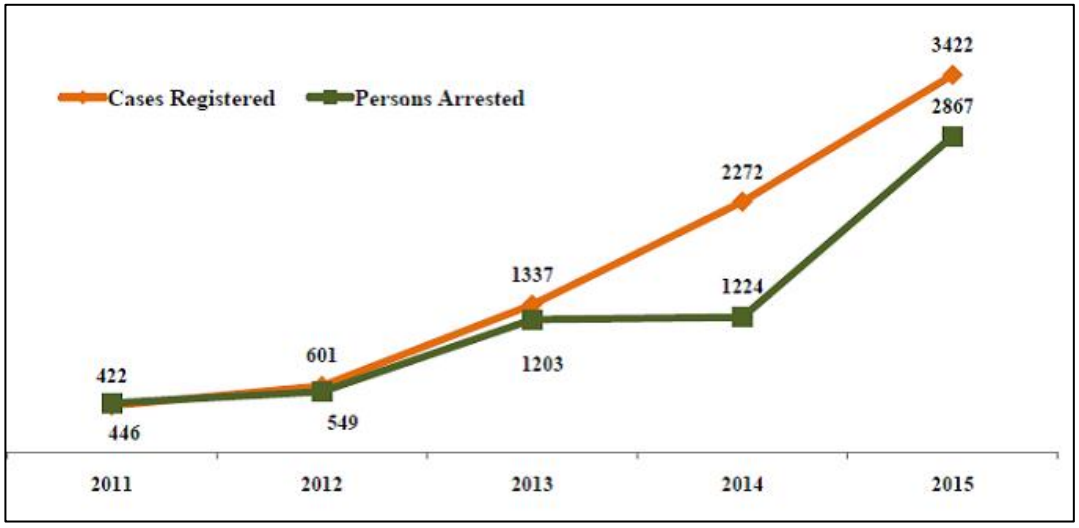


Figure 4: Cyber Crime in India- Cases Registered Under IPC Act (2011-15)

There are no surprises in the list of states with the highest rate of cybercrime from 2011 to 2015. With over 5900 incidents over the course of the five years, Maharashtra leads the list, followed by about 5000 cases in Uttar Pradesh. Third place goes to Karnataka with around 3500 cases. The states with the highest number of internet subscribers are at the top of this list. The bottom 10 are relatively smaller states with lower population & lower internet penetration.

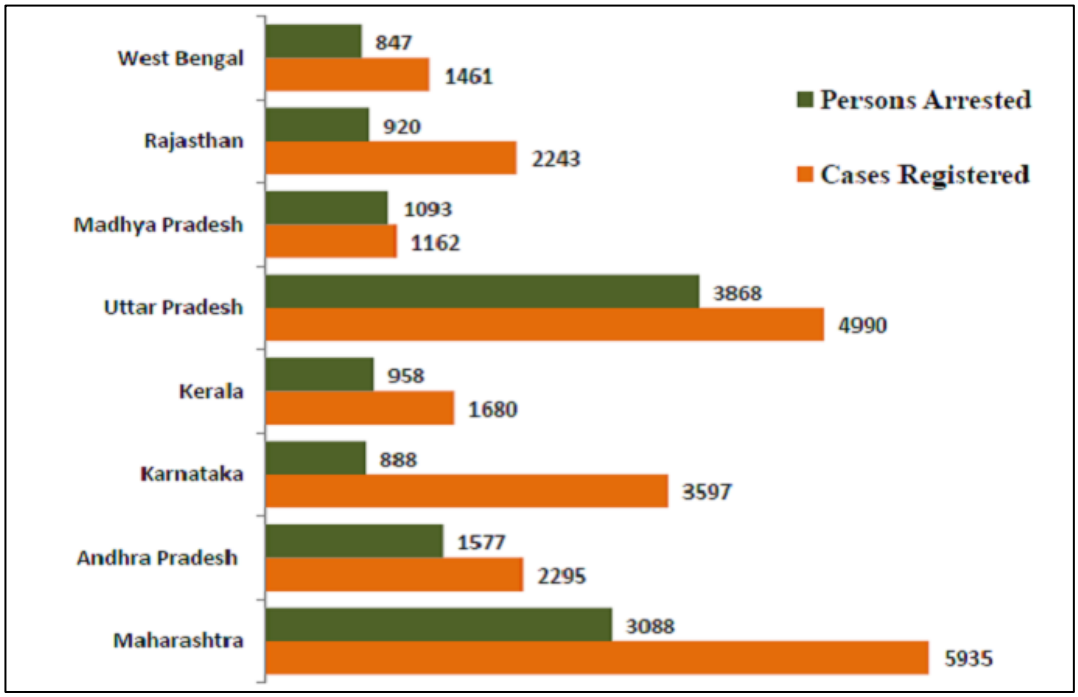


Figure 5: Cyber Crimes in States (2011 to 2015) [14]

Conclusion:

It is imperative that we recognize that criminals will persistently devise innovative techniques that capitalize on weaknesses in digital payment systems. It is therefore imperative that clients take precautions and stay up to date on the latest fraud prevention guidelines. Adopting a comprehensive strategy that incorporates policy, training, technology, and compliance, governments may create a digital environment that is safer. Significant progress has been made in India as a result of the the nation's digital transformation, but there is also an increasing danger of fraud and other cyberattacks. There has never been a greater need for strong cybersecurity safeguards, enhanced public awareness, and continued cooperation between the public and private sectors. India has the ability to create a safe and robust digital future by taking on these difficulties head-on.

References:

1. R. Sarath, K. Boddu, and V. R. Bendi, “Cyber Crime and Security, a Global Vulnerable Coercion: Obstacles and Remedies,” vol. 7, no. 5, pp. 5–8, 2017.

2. C. MOUNTAIN VIEW, “Symantec Announces MessageLabs Intelligence 2010 Annual Security Report.” [Online].
3. S. Alotaibi, A. Alruban, S. Furnell, and N. Clarke, “A Novel Behavior Profiling Approach to Continuous Authentication for Mobile Applications,” no. February, 2019.
4. C. E. Notar, S. Padgett, and J. Roden, “Cyberbullying: A Review of the Literature,” vol. 1, no. 1, pp. 1–9, 2013.
5. E. Abu-shanab, “Security and Fraud Issues of E-banking,” vol. 2, no. 4, pp. 179–187, 2015.
6. Holt T.J. & Bossler A.M. (2016). Cybercrime in Progress: Theory and prevention of technology enabled offenses. Routledge.
7. Clough, J. (2010). Principles of Cybercrime. Cambridge University Press.
8. Kesharwani, Subodh, Madhulika P. Sarkar, and Shelly Oberoi. "Cyber security in India: threats and challenges." Cybernomics 1.2 (2019): 32-34.
9. "Senate to probe rise in child cybersex trafficking". The Philippine Star. 11 November 2019.
10. "Global taskforce tackles cybersex child trafficking in the Philippines". Reuters. 15 April 2019.
11. "Webcam slavery: tech turns Filipino families into cybersex child traffickers". Reuters. 17 June 2018.
12. "How the internet fuels sexual exploitation and forced labor in Asia". South China Morning Post. 2 May 2019.
13. Veenoo Upadhyay, Dr. Suryakant Yadav, “Study of Cyber Security Challenges Its Emerging Trends: Current Technologies”5 IJERM 2349-2058 (2018).
14. "1st Session, 42nd Parliament, Volume 150, Issue 194". Senate of Canada. 18 April 2018.