RESEARCH ARTICLE OPEN ACCESS

Cybercrime Complaints across the Globe: An Empirical Examination of Patterns and Proliferation

Mallikarjun Konnur*
* Department of Commerce & Management, BLDEA's Commerce, BHS Arts and TGP Science College, Jamakhandi, Karnataka state, Email: mallusk2009@gmail.com

--************************----------------------------------

Abstract:

Cybercrime has become one of the biggest and most dynamic enemies the world has had to deal with in an age of digital connectedness. The research analyzes the trends and expansion of cybercrime complaints across the globe between 2019 and 2023, according to the information of the FBI Internet Crime Complaint Centre (IC3). With the help of a descriptive research design and secondary data analysis, this study classifies and determines the number of cybercrime types by using phishing, data breaches, extortion, and tech support scams. The results indicate an escalating rise in complaints, with a jump to an astonishing level, 467,361 complaints in 2019, and 880,418 complaints in 2023, emphasizing the exposure of people and organizations to digital space threats. The most common reported crimes are phishing and spoofing, personal data breaches, and e-commerce fraud. To a great extent, this intensification is based on the COVID-19 pandemic, which led to increased digital dependency. Trend analysis, which is expressed year-wise and category-wise, highlights the increasing number of traditional cyber threats and sophisticated attacks such as ransomware and SIM swapping. The article establishes an outstanding research barrier in the form of international, longitudinal reviews of online crime complaints and finds this challenge by offering an all-inclusive, multi-group review. It highlights the importance of powerful international cyber regulations, improved digital literacy, improved security systems, and international cooperation. The results can be used by policymakers, cyber security specialists, and stakeholders as they use a data-driven basis to formulate effective countermeasures. In conclusion, the study is part of an in-depth picture of the dynamic cyber threat environment and its importance to worldwide response, not only as a nation but also as a community.

Keywords —**Cybercrime, Phishing, Ransomware, Data Breach, Cybersecurity Policy & Complaint Statistics**

--************************----------------------------------

1. INTRODUCTION

1.2 Background of the Topic

In the age of digitalization, the internet is viewed as a significant part of our everyday lives as it helps us communicate, conduct trade, and share information across different boundaries. Nonetheless, the increasing cyberspace has also led to an astonishing increase in cybercrime, like phishing, identity crimes, data hacks, extortion, and ransom attacks (Holt et al., 2020). These malicious activities take advantage of technology flaws and human behaviour to do tremendous monetary, emotional and social damage. The development of the COVID-19 pandemic significantly accelerated the growth of online activities, accidentally providing the perpetrators with more possibilities to attack individuals and organizations (Lallie et al., 2021).

1.2 Importance of the Study

Since cybercrimes are becoming more complex and widespread, it is high time that we have data-driven knowledge of global cybercrime trends. Most current research deals with certain nations or selective crime categories without reflecting the global and chronological panorama (Wall, 2007). The issue of cyber security is related to understanding the trends and changes in cybercrime over time to provide timely responses to cyber security strategies, raising awareness amongst the citizens and aiding international cooperation (Singer & Friedman, 2014).

1.3 Objectives/Purpose of the Research

The main aim of the research is to examine the patterns of cybercrime complaints worldwide over five years (20192023) about the number and the nature of the crimes reported. This research aims to categorize the key cyber threats, define the new trends, and compare the changes in criminal activity based on secondary data provided by sources like the Internet Crime Complaint Center (IC3) established by the FBI.

1.4 Problem Statement / Rationale

Despite the range of annual cybercrime statistics published by different agencies, no gap in academic research that would put forward long-term multi-category trends on a global scale has been met so far. Most of the literature is limited to specific case studies or fails to compare years and various types of crime (Bada, Sasse, & Nurse, 2019). The paper fills this gap and conducts a trend-based study of cybercrime complaints based on a list of categories. The findings could be used to improve policy formulation, enhance cyber security practices and create focused awareness to counter the changing trends in digital threats.

2. LITERATURE REVIEW

Hackers have become one of the biggest threats to the digital infrastructure and the personal security of many people globally, with cybercrime being the most important problem in the domain. According to a Holt et al. (2020) study, there is an emerging sophistication of cybercrimes globally, mainly phishing, identity theft, and ransomware. Speaking about the impact of cybercrime on citizens' national security and privacy, Singer Friedman (2014) drew attention to the role of national awareness and the changes to the legal framework.

Bada, Sasse, and Nurse (2019) concentrated on the human issue in the context of cyber security breaches. He found that inadequate awareness and digital hygiene are some of the primary problems that lead to increased cybercrime. Likewise, FlorÃªncio and Herley (2013) conducted analyses and detection of password-related vulnerabilities, where they stated weak authentication actions to be the primary issue in personal data breaches.

An increase in cybercrime after the COVID-19 has become a hot topic. The study introduced by Lallie et al. (2021) entailed the pandemic-specific list of technological support scams, fraud scams, and impersonation-based attacks, which rose in numbers related to digital activity uptake during lockdowns. Finally, Button et al. (2020) also noticed how fraudsters immediately responded to trends connected with the pandemic, attacking individuals and organizations through phony relief programs and misleading health information.

Policy and regulation-wise, Wall (2007) criticized the inability of the prevailing laws to deal with the rapidly changing digital threats, especially in cross-border articles. The necessity to create an international, coordinated cyber security policy was also stressed by Chertoff and Simon (2017) to fight the existing transnational network of cyber criminals.

All these studies point to the same proximity of attention monitoring, legal mechanisms, and education to help combat cybercrime efficiently. Nevertheless, most current literature aims at a specific country, a particular type of cyber threat, or a limited period.

3. RESEARCH GAP

All the information notwithstanding, no comprehensive global analysis covering complaint trends in various types of crime against the backdrop of five years has yet been done. The available studies do not achieve a statistical comparison of the crime types and their development. The present research addresses the research gap as it examines the global data of cybercrime complaints in 20192023, providing a broader and more current viewing angle.

4. RESEARCH METHODOLOGY

The current paper will be based on the descriptive research design as it examines the global trends of cybercrime and the number of complaints. The primary purpose is to learn the nature, frequency and changes in the different types of cybercrime within five years. This research geography is the world, and the research gathers global complaint information based on some credible authorities. The statistics are pulled primarily based on the results of the Federal Bureau of Investigations Internet Crime Complaint Center (IC3) reports between 2019 and 2023. It involves using secondary data based on annual statistical reports published by the authorities.

The sampling design used is non-probability and purposive since the complaint records on cybercrime are classified annually. There was no primary sampling engagement, such as individual respondent units. As an alternative, the types of cybercrime complaints were analyzed, including complaints of key cybercrime (e.g., phishing, data breaches, extortion). The data collection instrument entailed a step-by-step gathering of statistics and tabulation of information provided in published reports.

The data analysis methods were trend analysis, frequency distribution, and year-wise comparison of the volume of complaints. The key shifts to crime types were interpreted with the help of graphs and tables. The results give us the quantitative foundation for the emerging cyber threat environment. Such methodology assures unbiasedness, applicability and broad generality of outcomes.

5. RESULT & DISCUSSION

Comprehensive Analysis of Cybercrime Trends and Complaint Statistics over the Last Five Years across the globe

Table 1 Types Of Complaint Statistics Over The Last Five Years Across The Globe

Crime Type	Complaints	Crime Type	Complaints
Phishing/Spoofing	2,98,878	Other	8,808
Personal Data Breach	55,851	Advanced Fee	8,045
Non-payment/non-delivery	50,523	Lottery/Sweepstakes/Inheritance	4,168
Extortion	48,223	Overpayment	4,144
Investment	39,570	Data Breach	3,727
Tech Support	37,560	Ransomware	2,825
BEC	21,489	Crimes Against Children	2,361
Identity Theft	19,778	Threats of Violence	1,697
Confidence/Romance	17,823	IPR/Copyright and Counterfeit	1,498
Employment	15,443	SIM Swap	1,075
Government Impersonation	14,190	Malware	659
Credit Card/ Check Fraud	13,718	Botnet	540
Harassment/Stalking	9,587	Real Estate	9,521

Source: Federal Bureau of Investigation Internet Crime Report 2023

The information given in the table 1 indicates that there are diverse forms of cybercrimes, and their prevalence depends on the number of complaints made. The most common categories of cybercrimes are phishing and spoofing, which dominate the statistics, respectively, with 298,878 complaints. Such crimes usually include fraudulent or deceptive emails or messages designed to cause people to spill information on passwords and financial accounts.

The personal data breach is followed by 55,851 complaints, demonstrating that the risk of unauthorized access to personal data remains high regardless of the data sender. That tendency reveals more weaknesses in data storage planning and increases the influence of cyber attacks on personal data. The number of people complaining of non-payment and non-delivery scams is 50,523, which shows how risky online buying and e-commerce fraud can be, especially at the peak shopping time.

There were 48,223 complaints of the extortion type, and they testify to the emergence of threats about ransom ware attacks and extortion schemes based on intimidation with payments to the victim. Thirty-nine thousand five hundred seventy complaints are registered in investment fraud related to increase Internet use to persuade victims in schemes claiming high investment returns. Compared to the 37,560 complaints reported, Tech support scams still target and victimize a person by posing as critical service providers, stealing information, or asking for payments to remedy falsely offered services.

Business Email Compromise (BEC) highlights with 21,489 complaints, which shows its effect on

and SIM swapping, signal developing criminal practices. To deal with them, technological security measures, education activities, and law enforcement solutions should be deployed to diminish the exposures and limit the effects.

The numbers indicate the increased complexity and variety of personal or corporate cyber attacks. Existing threats of phishing, data breaches, and

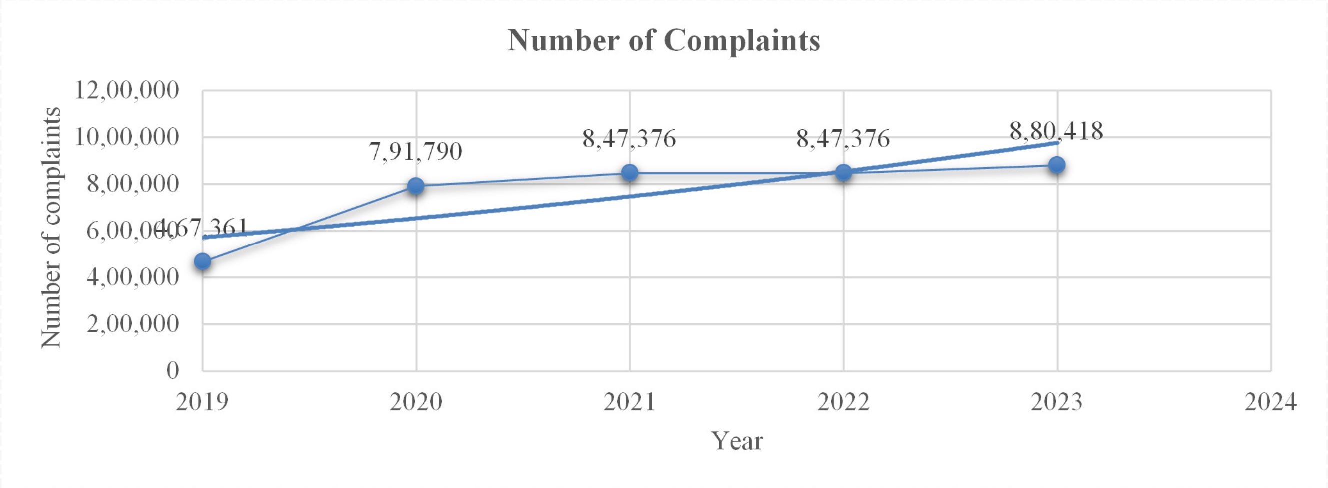
the organizations, as many fraudsters gain access to email messages and use them for financial theft. The grievances that made it to the top 20, such as identity theft with 19,778 complaints, remind us about the ongoing danger of misappropriating personal information by unscrupulous elements to conduct fraud. Confidence and romance scams, with 17,823 complaints, tell how the scammers apply emotional effects to fleece the victims, and, in many cases, they monetarily lose to a considerable degree. There has also been an increase in exploitation using employment scams, with 15,443 complaints, where job seekers are promised phony employment opportunities. The government impersonation scams that count 14,190 complaints rely on the trust in authority figures to lure them into providing personal and financial information. Additional notable categories entail credit card and check (13,718 complaints), harassment and stalking (9,587 complaints), and crimes that are characterized by threats of violence (1,697 complaints). Among the crimes that are not as common but equally worrying are ransomware attacks (2,825 complaints) and data breaches (3,727 complaints) that illustrate the necessity to improve cyber security defences. Cyber threats are changing and include intellectual property and copyright abuse (1,498 disclosures), SIM swapping (1,075 disclosures) and malware intrusions (659 disclosures). The statistics point to the fact that cybercrimes, regarding their sophistication and versatility, are on the rise and target different individuals and organizations. The most popular threats are phishing, data breaches, and extortion, whereas new types of threats, such as ransomware

extortion are still leading, and new waves of crime, such as ransomware and SIM swapping, show that there are new methods of criminals. MITIGATION: These problems must be addressed by combining technological solutions, awareness-raising measures, and law enforcement action to decrease susceptibilities and minimize the effects.

Table 2 Complaint Statistics over the Last Five Years across the Globe

Year	No of Complaints
2019	4,67,361
2020	7,91,790
2021	8,47,376
2022	8,47,376
2023	8,80,418
Total	**38,34,321**

Source: Federal Bureau of Investigation Internet Crime Report 2023



As per the information given in the table 2, the complaint statistics over the past five years demonstrate a progressive rise in the complaints given to the Internet Crime Complaint Centre (IC3). There were 467,361 complaints in 2019, but according to the statistics, the figure increased drastically to 791,790 in 2020. Such a sharp change (almost 70 percent) can be explained using the so-called effect of the COVID-19 pandemic, which fostered the transition to online operations (thus, due to the significance of this online switch, more people and organizations became exposed to cyber dangers). The situation remained the same in the coming years, with 847,376 complaints in 2021 and 2022. In 2023, the complaints were even higher at 880,418, the highest recorded number in five years.

There were 3,834,321 complaints during this period, signifying that internet crimes are persistent and increasing worldwide. The statistics illustrate the proliferation of online crimes and frauds; however, the sophistication of computer-related crimes, such as phishing, ransomware, and identity theft, also unlawfully attacks a victim. The fact that the complaints will remain high in 2021 further stresses that cyber threats have become a constant challenge and should be treated as one.

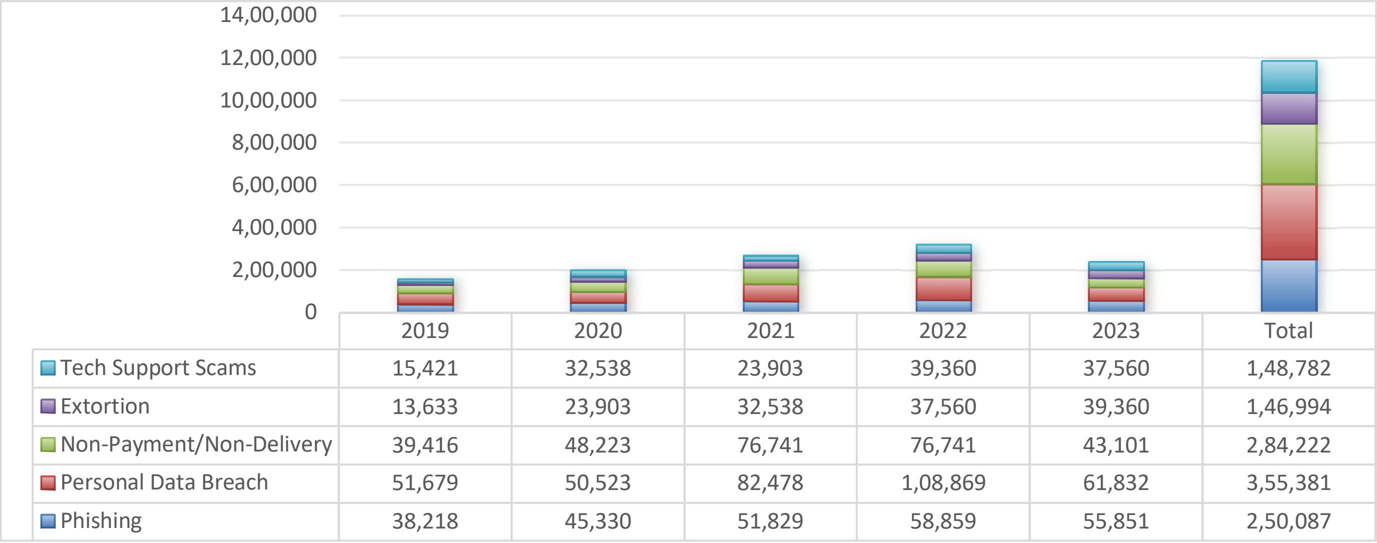
The trend highlights the significance of implementing robust cyber security activities and raising awareness among the population to ensure they can overcome cybercrime risks. The trend in the rising complaints indicates that more measures, such as sturdy legal frameworks, an advanced monitoring system, and an incident reaction system, must be implemented to help protect individuals and businesses in the face of the new threats. Internet crimes are only increasing, not abating, and the need to practice vigilance and undertake preventive strategies will always be essential to mitigate these crimes' effects and eliminate more vulnerability.

This table captures cybercrime trends and indicates the variability of specific categories, including phishing, personal data breaches, non-payment/non-delivery scams, extortion, and even tech support fraud. It is important to note that personal data breaches reached their highest level in 2022. Still, phishing and non-payment/non-delivery fraud showed the most significant activity in previous years and slightly decreased in 2023. Cases of extortion had a consistent upward trend, and the use of digital threats can be considered a factor that contributed to this trend, whereas the number of tech support scams was also on the constant rise as time passed

Phishing	Personal Data Breach	Non-Payment/ Non-Delivery	Extortion	Tech Support Scams
38,218	51,679	39,416	13,633	15,421
45,330	50,523	48,223	23,903	32,538
51,829	82,478	76,741	32,538	23,903
58,859	1,08,869	76,741	37,560	39,360
55,851	61,832	43,101	39,360	37,560
2,50,087	3,55,381	2,84,222	1,46,994	1,48,782

Table 3 Top Five Crime Types Compared Over the Last Five Years across the Globe

Source: Federal Bureau of Investigation Internet Crime Report 2023



	2019	2020	2021	2022	2023	Total
🟦 Tech Support Scams	15,421	32,538	23,903	39,360	37,560	1,48,782
🟪 Extortion	13,633	23,903	32,538	37,560	39,360	1,46,994
🟩 Non-Payment/Non-Delivery	39,416	48,223	76,741	76,741	43,101	2,84,222
🟥 Personal Data Breach	51,679	50,523	82,478	1,08,869	61,832	3,55,381
🟦 Phishing	38,218	45,330	51,829	58,859	55,851	2,50,087

6. CONCLUSION AND SUGGESTIONS

Analyzing the world of cybercrime complaints between 2019 and 2023, one must admit that there is a stable and threatening increase in the level and range of complaints concerning cybercrime. Phishing and spoofing have become the most common cybercrime, next to personal data breaches, non-payment/non-delivery scams, extortion, and tech support fraud. The statistics also show that the number of complaints has grown considerably during the COVID-19 pandemic, which was caused by the intensified internet use and reliance on digital technologies, thus presenting additional opportunities. Although certain crime types have attested changes over the years, the direction of this trend is toward the increasing sophistication and persistence of cyber threats experienced globally. These findings are vital as far as policy and enforcement of cyber security are concerned. The fact that the complaints only grow proves the severe necessity of solid legal frameworks, high-quality cyber security systems, and mass education. Cybercrime is a technological problem but also a social, economic and geopolitical problem. Therefore, there must be a coordinated effort to deal with these global issues and international collaboration. Given the findings, the policymakers should reinforce international law structures and uniform cyber laws to seal the jurisdictional lapses. Law enforcement agencies should invest in training and providing digital forensic abilities to investigate complex crimes. Companies in finance, healthcare, and e-commerce must implement multi-level security measures and carry out risk-based assessments. Increased publicity campaigns need to be done to sensitize users on phishing, internet scams and the security of personal information. Last but not least, there is a need to conduct additional academic studies devoted to analyzing cybercrime at the regional level, profiling cyber offenders and the efficiency of existing cyber security policies in different countries.

7. REFERANCES

Journal Articles and Conference Papers

1. Bhalla, A. (2019). “Cybercrimes in Indian Web Applications: Web Jacking and Mitigations.” *International Journal of Cyber Law*, 7(1), 92-103.
2. Dr.Chidanand Byahatti, Mr. Mallikarjun Konnur. (2025). Determinants of Market Volatility in the Indian Stock Exchange: A Case Study of the Bombay Stock Exchange (BSE). In IJSRED - International Journal of Scientific Research and Engineering Development (Vol. 8, Number 1, pp. 1260–1268).Zenodo.https://doi.org/10.5281/zenodo.15032370
3. Pandey, A., & Gupta, M. (2020). “Botnet Detection Techniques in India.” *International Journal of Computer Networks & Communications*, 12(1), 45-56.
4. Gupta, B., Tewari, A., & Sharma, A. (2018). “Cyber Attacks and Preventive Defense in Indian Organizations.” *Journal of Information Security and Applications*, 40, 87-95.
5. Böhme, R., & Schwartz, G. (2010). “Modeling Cyber-Insurance: Towards a Unifying Framework.” *Workshop on the Economics of Information Security (WEIS).*
6. Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2012). “The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes.” *IEEE Symposium on Security and Privacy*, 553-567.

7. Kumar, D. (2020). “Exploring Vishing in India: A Review of Cases.” *International Journal of Cybersecurity*, 6(2), 113-125.
8. Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). “Social Phishing.” *Communications of the ACM*, 50(10), 94-100.
9. Sharma, K., & Kapoor, S. (2020). “Analysis of Malware Attacks in India."*International Journal of Information Security*, 19, 123-137.
10. Kharraz, A., Robertson, W. K., Balzarotti, D., Bilge, L., & Kirda, E. (2015). “Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks.” *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, 3-24.
11. Jha, M., & Tiwari, R. (2020). “Denial of Service Attacks in India: Current Trends.” *Journal of Network and Computer Applications*, 149, 23-36.
12. Tandon, M. (2020). “The Rising Trend of Cyber Stalking in India.” *Indian Journal of Law and Technology*, 15, 84-101.
13. Agarwal, N. (2020). “Internet Time Theft in Indian Workplaces: A Growing Concern.” *Journal of Cyber Law and Employment Studies*, 4, 41-58.
14. Ozment, A., & Schechter, S. E. (2006). “Milk or Wine: Does Software Security Improve with Age?” *USENIX Security Symposium.*
15. Chauhan, P. (2020). "XSS Vulnerabilities in Indian Web Applications."*Journal of Computer Virology and Hacking Techniques*, 16(3), 211-225.
16. Singh, P. (2020). "Web Jacking in India: Methods and Prevention."*Journal of Information and Cyber Security*, 5(2), 34-42.
17. Deka, R. (2018). "Domain Name Disputes and Cyber Squatting Cases in India."*Indian Journal of Law and Technology*, 13, 201-220.
18. Mehta, R. (2019). "Trojan Attacks in Indian Organizations: Trends and Solutions."*Journal of Cyber Security and Privacy*, 2(3), 178-188.
19. Singh, R., & Saini, S. (2019). "Phishing Attacks on Indian Banking Sector: A Review of Trends."*Journal of Cyber Security and Privacy*, 2(2), 128-145.
20. Agrawal, S., & Sharma, A. (2020). "Cyber security and Hacking Trends in Indian Enterprises."*International Journal of Information Technology*, 12(3), 21-35.
21. Bose, S., & Mitra, A. (2019). "Cyber security Threats and Botnet Infections in India."*Journal of Cyber Security*, 6(3), 213-225.
22. Gupta, S. (2019). "DoS and DDoS Attacks on Indian Financial Institutions: A Review."*International Journal of Information Security Science*, 8(2), 44-52.
23. Joshi, S., & Dubey, R. (2020). "Cross-Site Scripting Attacks in India: Mitigation and Challenges."*International Journal of Information Security*, 18, 421-434.
24. Mishra, S. (2020). "Workplace Productivity and Cyber Issues: Internet Time Theft.” *Asian Journal of Management Cases*, 16(2), 138-145.
25. Srivastava, S., & Bajpai, R. (2019). “Cyberstalking in India: Legal Challenges and Responses."*International Journal of Cyber Criminology*, 13(1), 21-35.
26. Sundaram, S., & Harsha, M. (2020). "Financial Phishing Attacks in India.” *Asian Journal of Cyber Law*, 2(1), 102-110.
27. Thakur, S. (2020). "Impact of Email Bombing on Indian Institutions."*Journal of Computer Security*, 28(4), 95-104.
28. Verma, S. (2020). "Voice Phishing (Vishing) in India: Emerging Threats."*Journal of Financial Crime*, 27(4), 1241-1251.
29. Bansal, V. (2019). “Cybersquatting in India: Legal Challenges and Dispute Resolution

Mechanism."*Journal of Intellectual Property Rights*, 24, 32-41.

30. Patel, V., & Singh, N. (2020). "Email Bombing as a Cybercrime in India: Legal Perspectives."*Journal of Information Security and Applications*, 42, 101-111.

Reports and Websites

1. Bonneau, J., Anderson, R., & Danezis, G. (2012). *The quest for secure online identities. Communications of the ACM.*
2. Chakrabarti, R., & Manoharan, P. (2020). *Cyber security challenges in the developing world. Journal of Cyber Policy.*
3. Cyber security Ventures. (2022). *Cybercrime report.*
4. FBI IC3. (2023). *Internet crime report 2023.*
5. NCRB. (2023). *National Crime Records Bureau Annual Report.*
6. Ponemon Institute. (2023). *Cost of data breach report 2023.*
7. Sharma, N., & Singh, R. (2021). *Impact of awareness programs on reducing phishing attacks. Cyber Defense Journal.*
8. Verizon. (2022). *Data breach investigations report.*
9. National Crime Records Bureau (NCRB). *Annual Report.*
10. Indian Computer Emergency Response Team (CERT-IN). *Cyber security Threat Report.*
11. PwC Cyber Security Insights. *Cyber security Survey.*
12. Indian Cyber Crime Coordination Centre. *Annual Report.*