IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Digital Era-Development Path Or Victim Of Cybercrime: An Empirical Study

Khushboo Patel
Research scholar, Kalyan P.G. College Bhilai, Affiliated to Hemchand Yadav Vishwavidyalaya Durg (C.G.)
Email:

Vimal kumar Patel
Research scholar, Kalyan P.G. College Bhilai, Affiliated to Hemchand Yadav Vishwavidyalaya, Durg (C.G.)

Harsha Sirmour
Research scholar, Kalyan P.G. College Bhilai, Affiliated to Hemchand Yadav Vishwavidyalaya Durg (C.G.)

Abstract

Purpose- The purpose of this paper is to identify the level of awareness towards internet security measures, cyber security, and cybercrimes in digital era.

Research Methodology- This research starts with the conceptual framework of digitalization in India and it mainly focuses on cyber security. Both primary and secondary data are used and convenience sampling has been done with a total sample size of 320.

Findings- The study disclosed that the awareness level among the respondents is very low and only a few respondents have knowledge about internet security measures that helps them from cybercrimes. So that the govt can work on these factors and the appropriate measures can be taken by them.

Research Limitations- The study area is limited to the Durg district only due to lack of time. In future the researchers may explore each type of cyber fraud separately.

Implication- This research paper highlights the awareness among people towards cyber security and the way they dealt with cybercrimes.

As we know “Innovation creates the potential for exploitation.”

“People trust when they shouldn't.”

Keywords- Digital India, Cybercrime, Cyber victim

I. Introduction

In our digital era, innovations are made every day that make our lives easier but also introduce new challenges and worries. In the digital era, perfect security is more important than how technology will enhance. This research paper's goal is to emphasize the value of adopting a positive attitude toward technology as well as the precautions that may be done to shield ourselves from being victims of cybercrime. On August 15, 1995, Videsh Sanchar Nigam Limited (VSNL) introduced internet services, marking the beginning of India's journey in the digital world. When the internet first appeared, it broke down barriers to worldwide collaboration, engagement, and connectivity. And as time goes on, technical advancements in the digital world keep moving from networks of powerful computers to laptops, and now to our mobile phones, making it easier for people to complete things that previously required a lot of time and effort. Today, information access, selling, and buying have all become incredibly simple with just one click, we can obtain a wealth of knowledge in our hands on our devices and do all other tasks in a matter of seconds. The term crime is described as behaviour that violates official laws and which is punishable by formal sanctions. It is also defined as a criminal offense that is harmful not only to the individuals but also to the government, community, companies, state, and country.

The Digital India Vision

Three main categories form the core of the digital India vision. These are what they are:

1. As a service, digital infrastructure aims to give everyone a cradle-to-grave internet identity, a high-speed internet connection, a mobile phone a shared private area, access to a community service centre, and a bank account in a public cloud in a secure online environment.
2. Availability of on-demand services and governance in real-time for platforms for online and mobile use that are completely connected between departments and jurisdictions. All citizen documentation will be made available on the cloud platform, so residents won't be required to present them to use certain services. Additionally, the availability of cashless electronic transactions will aid in corporate growth. Systems for Geographic Information (GIS) be incorporated into the development plans.

3. Make citizens more capable by teaching them digital literacy, especially in rural areas. This will be accomplished by utilising cooperative digital platforms and by creating in order to facilitate access to the digital resources in their native tongue, their involvement became actual. It will facilitate access to openly available data.

The term crime is used to outline the activities which are done through computer networks, mobile phones, and different electronic devices. It encircles a different and wide range of crimes which include identity stealing, pornography, phishing, spoofing, etc. The very common types of cybercrimes are listed below;

i. Fraud in telecommunication services,
ii. Telecommunication piracy,
iii. Offensive material dissemination,
iv. Money laundering and tax evasion,
v. Terrorism and extortion,
vi. Sales and investment frauds,
vii. Telecoms illegal interception,
viii. Electronic Fund Transfer fraud.

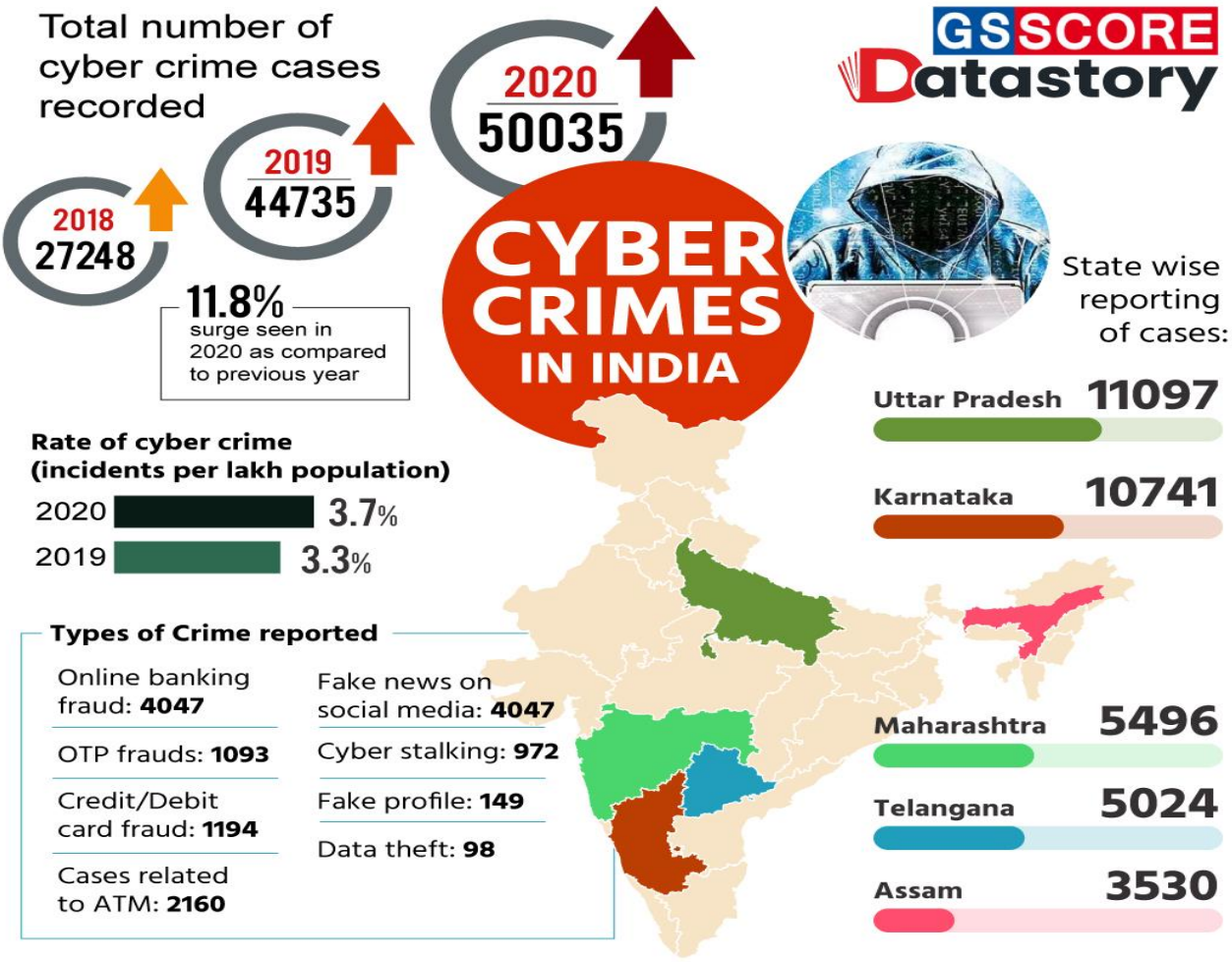
('Digital India Scheme,' n.d.) Computer technology has become entrenched in people's lives and the coexistence of users and electronic computing devices would be peaceful without the malicious actions of cyber criminals that could cause irreparable harm to the victims. The main purpose of this study is to draw attention to the special features of the virtual environment from the victim's dogmatic point of view. This study will help people to understand cybercrime- challenges, legal response, and, phenomena.

Some facts related to Cybercrimes in India

(Tanushree Basuroy, 2022) In India, there were more than 4.5 thousand reports of cybercrime including sexual harassment or exploitation in 2021. Compared to 2016 and 2017, there was a significant increase in these cybercrimes across the nation. The Indian government's attempts to build new procedures to address cybercrime, combined with increased public awareness, were some of the causes generating such a huge surge in reported occurrences of cybercrimes, even though the country's crime rate had increased from 2018 to 2020.

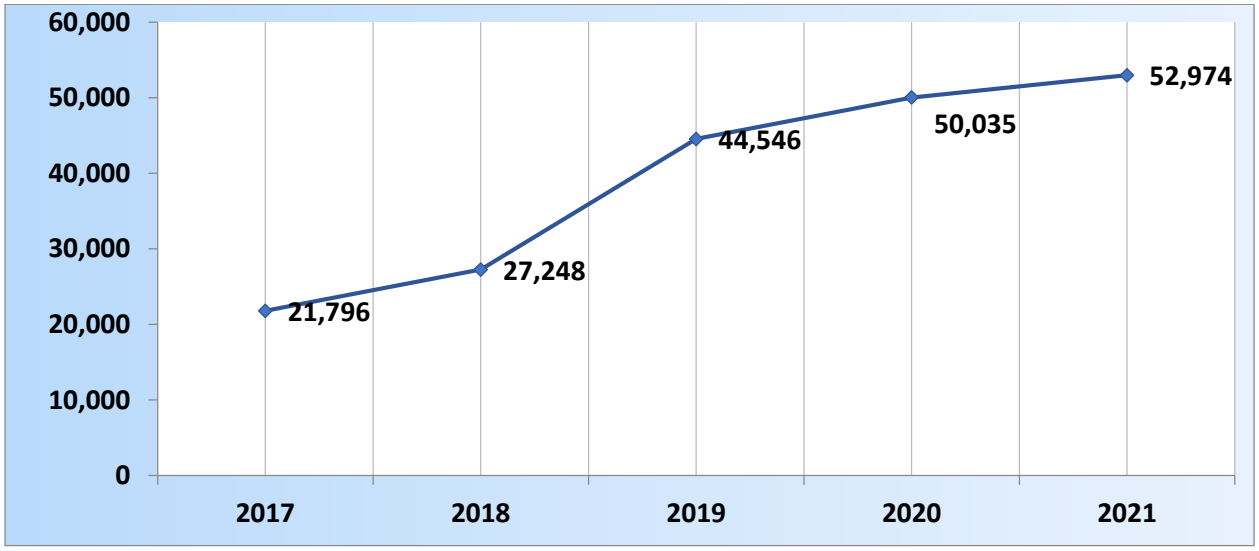
(Sandhya Keelery & Text, 2021) India, which has the second-largest internet user base in the world, was also a part of the expanding digital village. While the internet's increased connection offers widespread advancement, it also exposes our digital society to new threats. Cybercrimes are transnational and have developed at a rate equal to that of new technology. The number of cybercrimes recorded nationwide keeps rising at a noticeable rate each year.

Graph no. 1 Recent data related to Cybercrimes in India



Source: - (Cyber Crimes In India, 2022)

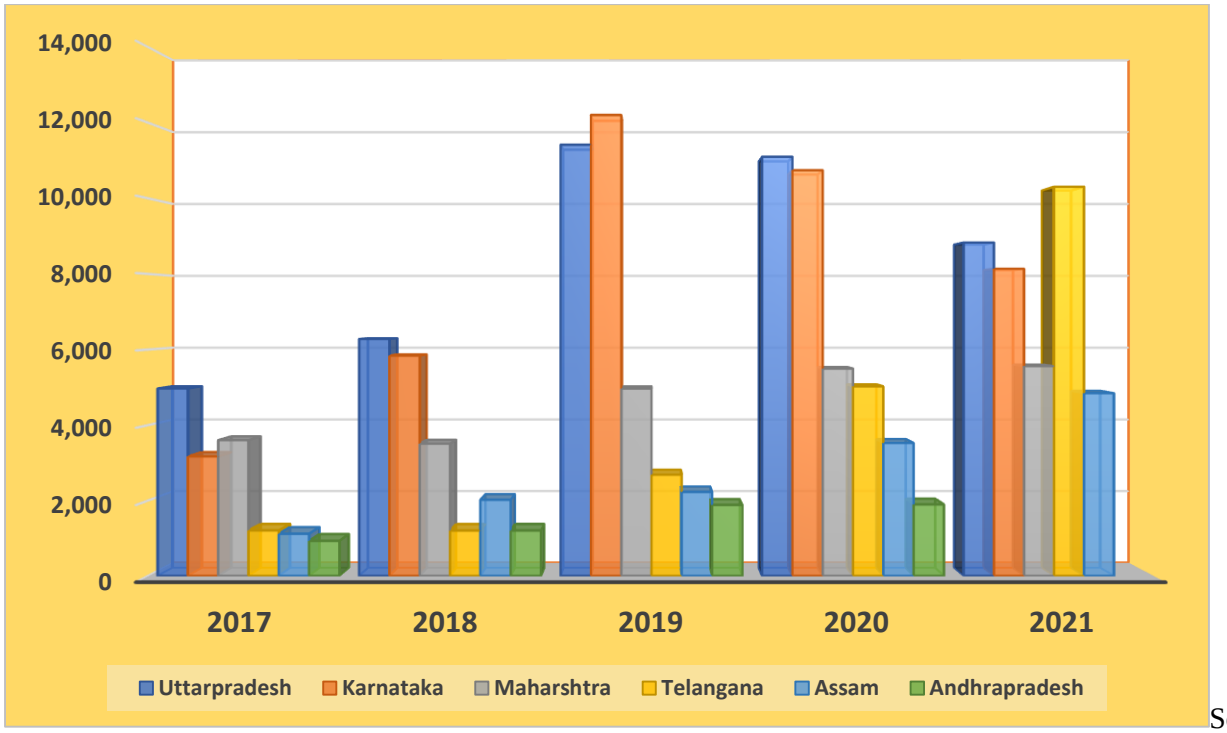
Chart no. 1 Total number of registered Cybercrimes in India past 5 Years From the below chart, we can find that in the year 2017 the total number of cybercrime cases registered was 21796, in 2018 it was 27248, after that in 2019 sudden increase in no. of cases 44,546, when it comes to year 2020 it was about 50,035 and in the year 2021, it was 52974.



Source:

- **National Crime Records Bureau (NCRB) data**

Chart no. 2 State-wise and Year-wise cybercrime reports in India



Source:

- **National Crime Records Bureau (NCRB) data**

The above bar graph shows the top 6 states of India which are hotspots of cyber criminals. In 2017 most of the cases are registered from Uttar Pradesh and the least were from Andhra Pradesh. Concentrating on 2018 most of the cases were registered from Uttar Pradesh and least from Telangana. Year 2019 shows the highest number of cases from Karnataka and the lowest from Andhra Pradesh. 2020, where the highest record was from Uttar Pradesh and the least from Andhra Pradesh. In the year 2021 highest cases were reported from Telangana and the least were from Andhra Pradesh.

II. Review of Literature

1. **(Esther Ramdinmawii, Seema Ghisingh, & Usha Mary Sharma, 2014)** Their study shows that every individual should have complete awareness regarding crimes and their judicial laws. They found a very common area of causing cybercrime is especially sales and investment. There are different types of fines and penalties which are enforced by the judiciary to help the people.
2. **(Megha Solanki, 2022)** studied that other than matriculation it should be taught to school students through different types of seminars, and webinars by IT professionals. The major concern in the present era is related to phone privacy and for this accessible knowledge is very important.
3. **(Khan, 2020)** found in his study that every person who is using the internet will have a threat that their data can be theft. As much as cyber security increases cybercrime also increases because cyber criminals always use loopholes to hack confidential locks and devices.
4. **(Ravishankar Ulle, Kotresh Patil, Dr. Aparna, Dr. Niraj Kumar, & Renuka Murthy, 2018)** studied that digitization brought transparency in work and paperwork get reduced. For strengthening digitalized economy every individual must have intellectual knowledge. An economy that is strongly digitalized shows better utilization of capital and develops much faster.

5. **(Dr. Giridhari Mohanta, Dr. Sathya Swaroop Debasish, & Dr. Sudipta Kishore Nanda, 2017)** made a study that our country is having a very strong and powerful infrastructure. The national economy will increase when youths were employed. The success of Digital India campaign will be successful only if every citizen supports it. There are many barriers too but we must look forward to our better and more successful implementation of the Digital India Campaign.

III. Significance/ Scope of the study

The research area of the study is limited to the Durg city of Chhattisgarh state. The study attempts to show the status of digitalized India, the digital divide, cybercrime, and awareness among people towards digital platforms and digital security. The study covers internet security measures, and awareness among respondents while using different types of digital platforms. The study will help us to know the awareness of people towards cybercrimes, cyber criminals, and the satisfaction level for cyber security measures while using the digital platform.

IV. Objective of the study

1. To study the development of the digital era and trend analysis of cybercrimes.
2. To determine the factors influencing people to adopt digital platforms & factors affecting cybercrime.
3. To evaluate the awareness level of the respondents towards cybercrimes and cyber security in digital era.

V. Hypotheses of study

1. H_{01} There is no association between registered cybercrimes and the volume of digital payments.
2. H_{02} Paperless work or environment friendly is not responsible for the adaptation of digital platforms.
3. H_{03} There is no significant difference between demographic factors and awareness level of cybercrime.
4. H_{04} Respondents are not fully aware of all the precautionary steps of cyber security.

VI. Research Methodology

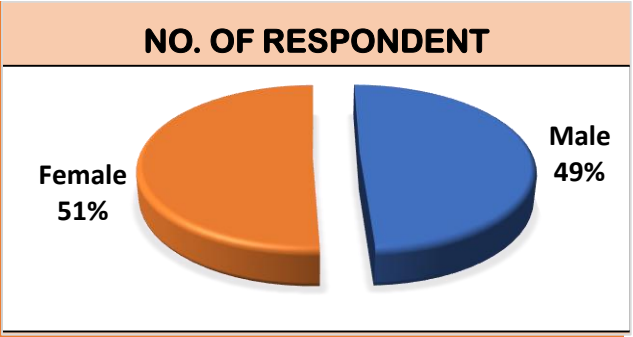
This study is focused on digitalization in India with special reference to the Durg district of Chhattisgarh. The first and foremost obstacle to getting digitalised is an internet security and cyber-attacks. This study is based on both primary and secondary sources of data collection. The convenience sampling method was adopted to collect the data and the sample size of the study is 320. The nature of this study is descriptive and empirical. Primary data was collected through a closed structured questionnaire using a 5-point Likert scale and data was compiled in the form of a table and graph. Some statistical tools chi-square and correlation were also used.

VII. Analysis & Interpretation

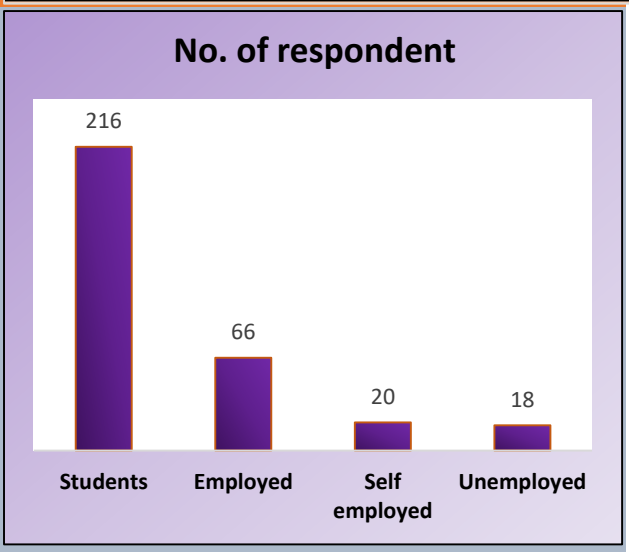
Section A Demographic profile of Sample

Study of demographic profile is essential for analysis. It includes age, gender, educational qualification, occupation of the respondents.

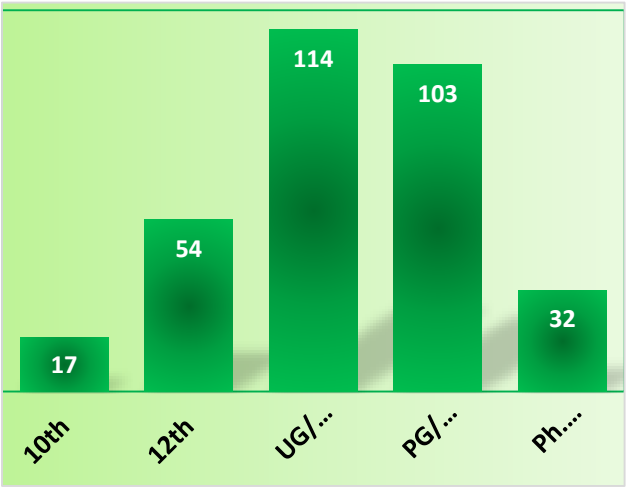
Gender	No. of respondent	
Male	158	49%
Female	162	51%
Grand Total	**320**	**100%**



Occupation	No. of respondent	
Students	216	68%
Employed	66	21%
Self-employed	20	6%
Unemployed	18	6%
Grand Total	**320**	**100%**



Educational Qualification	No. of respondent	
Up to 10th	17	5%
Up to 12th	54	17%
UG/ Graduate	114	36%
PG/ Postgraduate	103	32%
Ph.D. / Professional Degrees	32	10%
Grand Total	**320**	**100%**

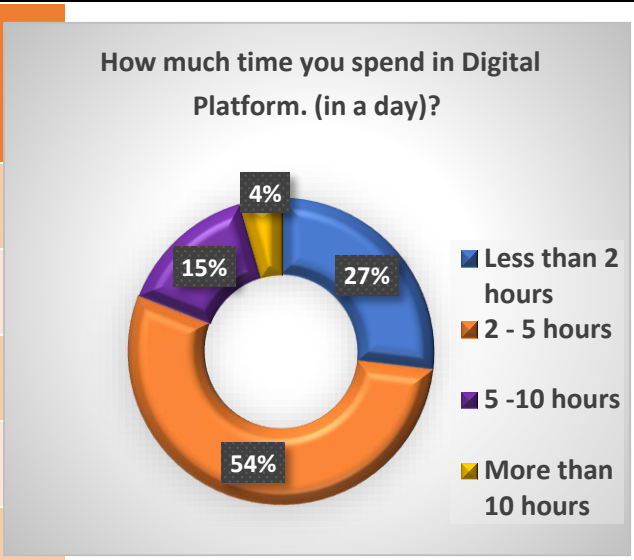


i.

Section B

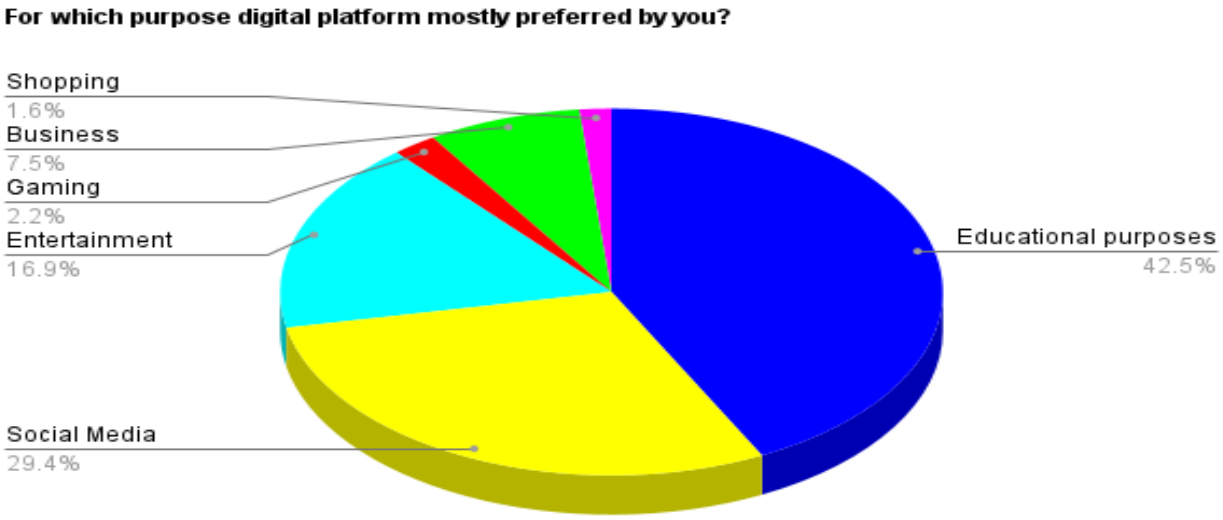
i. **Table no. 1** No. of hours spend in a day at Digital Platform. More than 50% spend 2-5 hours in a day.

	No. of respondent	
Less than 2 hours	**86**	**27%**
2 - 5 hours	**173**	**54%**
5 -10 hours	**47**	**15%**
More than 10 hours	**14**	**4%**
Grand Total	**320**	**100%**



ii. Table no. 2 Most of the time digital platforms used by respondent

For which purpose most of the time digital platforms used by respondent	No. of respondent
Business	24
Educational purposes	135
Entertainment	54
Gaming	7
Shopping	5
Social Media	95
Grand Total	**320**



Majority of the respondents (42.5%) were using for educational purpose, about 30% spending time on social media as favourite platforms for the young generation.

iii. Table no. 3- Availability of 24*7 internet connectivity

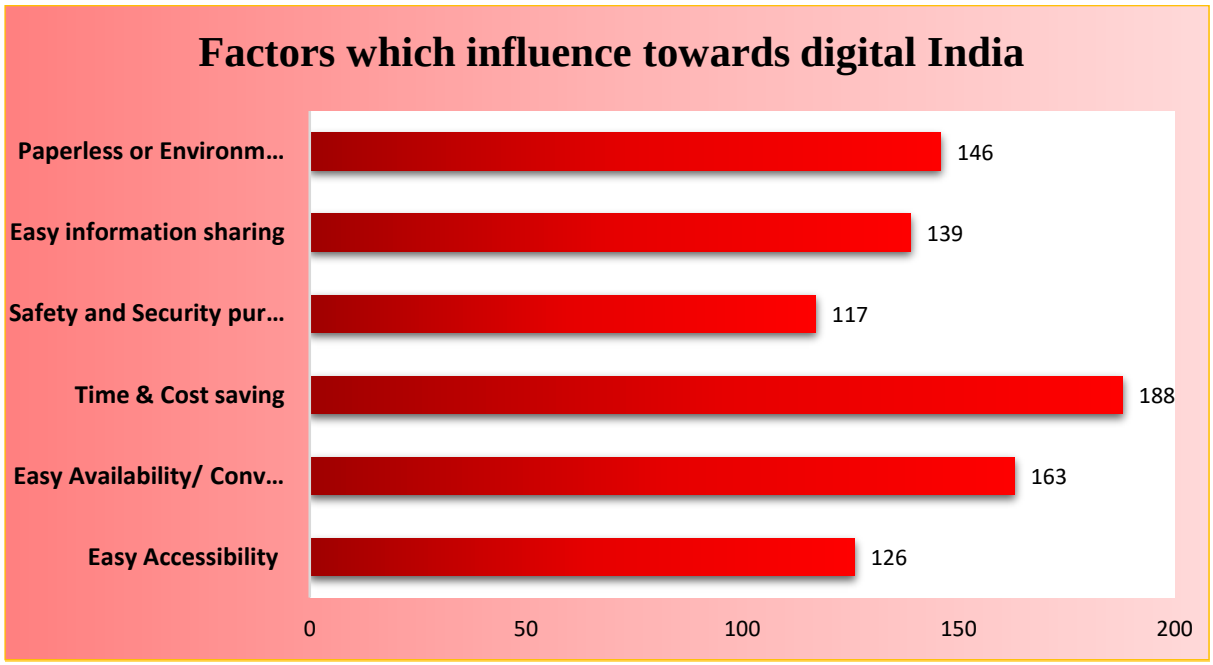
Is there 24*7 Internet connectivity in your locality	No. of respondent	
Yes	228	71%
Sometime	43	13%

For now, almost more than

No	49	15%
Grand Total	**320**	**100%**

70% have strong and 24*7 internet connectivity which is a good indication for the digital era. Still there is scope for the better internet facility in almost 30% which having poor internet connectivity.

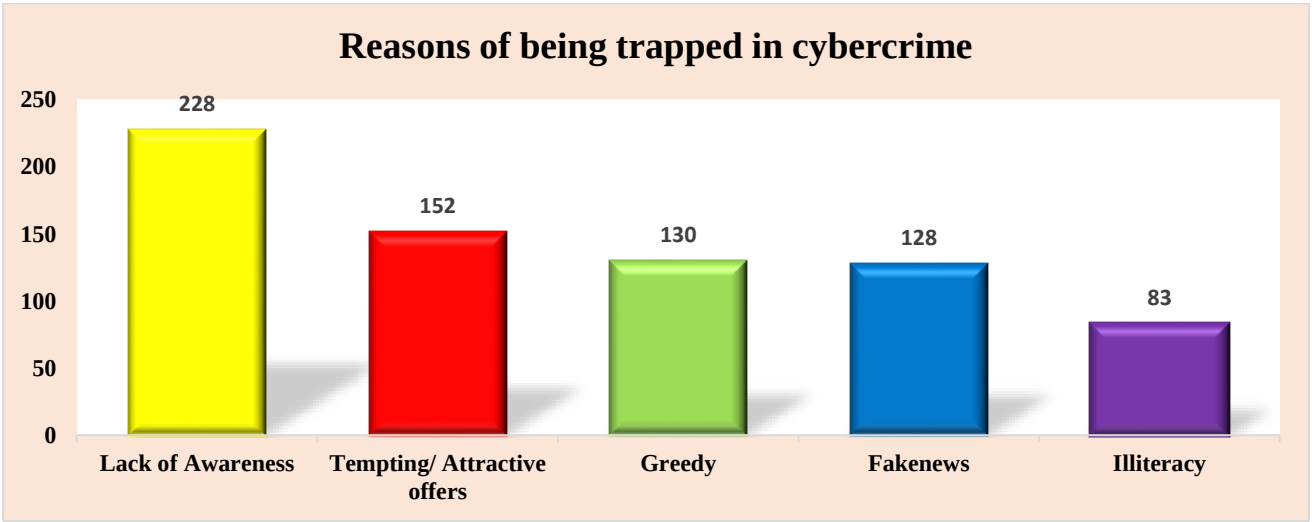
iv. **Table no. 4- Factors which influence people to be digitalized**



The above chart indicates that the factor which influence people to get themselves digitalised is time and cost saving. The least factor chosen by respondents is safety and security measures.

Section C - Cybercrimes and Cyber security in Digital Era

i. **Table no. 1** Reasons of being trapped in cybercrime, certain factors are considered like Lack of awareness is the mostly chosen by the respondents (about 70%). Tempting attractive offers, Greediness, using Fake news to deceive people. Lowest marked reason was Illiteracy as even now Educated people are falling in the trap of cybercrime



ii. **Table no. 2** Registered no. of cybercrimes and Total digital payments

Correlation between number of registered cybercrimes and total digital payments

Null Hypothesis (H_0): There is no correlation between number of registered cybercrimes and total digital payments.

Alternate Hypothesis (H_1): There is a correlation between number of registered cybercrimes and total digital payments.

Year	Registered no. of Cybercrimes	Total Digital payment (Volume)
2017	21,796	1,45,902
2018	27,248	2,34,339
2019	44,546	3,43,455
2020	50,035	4,37,445
2021	52,964	7,19,531

Test used: Karl Pearson correlation

Registered no. of Cybercrimes	**1**	
Total Digital payment (Volume)	**0.88**	**1**

As per the table, **correlation is 0.88** which indicates **a strong correlation between** the above variables. Hence the null hypothesis gets rejected & the alternative hypothesis is accepted. It also indicates that there is a positive correlation between number of registered cybercrimes and total digital payment (volume).

iii. Table no. 3 Confidence level of people towards security of personal devices & online accounts.

Confidence level of people towards security of personal devices & online accounts.	Gender				No. of respondent
	Male		Female		
Confident	**83**	**53%**	**87**	**54%**	**170**
Neither Confident nor unconfident	31	20%	48	30%	79
Unconfident	9	6%	8	5%	17
Very Confident	35	22%	17	10%	52
Very Unconfident	-	-	2	1%	2
Grand Total	**158**	**100%**	**162**	**100%**	**320**

Test Used Chi square Test statistics is used for analysis of educational qualification with security towards personal devices and online account**.**

Educational Qualification	Very Confident	Confident	Neither Confident nor unconfident	Unconfident	Very Unconfident	Grand Total
Up to 12th	8.78	28.69	13.33	2.87	0.34	**54**
Up to 10th	2.76	9.03	4.20	0.90	0.11	**17**
Postgraduate	16.74	54.72	25.43	5.47	0.64	**103**
Ph.D./ Profess. Degrees	5.20	17.00	7.90	1.70	0.20	**32**

Graduate	18.53	60.56	28.14	6.06	0.71	**114**
Grand Total	**52**	**170**	**79**	**17**	**2**	**320**
p-value <0.05	0.005556					
Chi-Square Test	0.999996					

As the P value (0.005) is lesser than 0.005 (level of significance), hence the null hypothesis has been rejected and alternate hypothesis is accepted. It means there is significant difference between the educational qualification and Confidence level while using personal devices & online accounts

iv. Table no. 4 Believe of people whether laws can control cybercrime.

Believe of people whether laws can control cybercrime.						
Gender	**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**	**Grand Total**
Male	13.33	43.94	60.73	32.09	7.90	**158**
Female	13.67	45.06	62.27	32.91	8.10	**162**
Grand Total	**27**	**89**	**123**	**65**	**16**	**320**
p-value <0.05	0.005556					
Chi-Square Test	0.999996					

Test Used

The Chi-square test is used to analyse the significant difference between male respondents and female respondents with respect to effectiveness of laws to control cybercrimes.

As the P value 0.005 is less than 0.05(level of significance), hence the null hypothesis has been rejected and alternate hypothesis is accepted. It indicates that there is significant difference between male and female respondent with regard to their believe on laws that can control cybercrime.

v. Table no. Frequencies of changing password for the security purpose.

Frequencies of changing password for the security purpose.	**Gender**					
	Male		**Female**		**Grand Total**	
Never	22%	35	27%	43	**24%**	**78**
Once in a month	41%	64	27%	44	**34%**	**108**
Once in a week	4%	7	5%	8	**5%**	**15**
Once in a year	33%	52	41%	67	**37%**	**119**
Grand Total	**100%**	**158**	**100%**	**162**	**100%**	**320**

Test Used

Chi square is used to analyse the association between gender and frequency of changes in password.

Gender	Never	Once in a month	Once in a week	Once in a year	Grand Total
Male	38.51	53.33	7.41	58.76	**158**
Female	39.49	54.68	7.59	60.24	**162**
Grand Total	**78**	**108**	**15**	**119**	**320**
P Value	If, p-value <0.05 H0 is rejected			0.092 H0 is Accepted	
Chi Square Value	0.993				

As the P value (0.092) is more than (0.05), hence the H_0 (null hypothesis) has been accepted and alternate hypothesis is rejected. It means there is no significance difference among genders while changing passwords for the security measures.

Section D

Awareness level regarding internet security measures in digital era

i. Table no. 1

1. Awareness regarding security measures while using internet?	No. of respondent	
Yes	242	76%
No	78	24%
Grand Total	**320**	**100%**

The table shows that 76% of respondents have awareness regarding the security measures and 24% of respondents accept that they are not aware.

ii. Table no. 2

2. Have you enabled Two- factor authentication for any of your online accounts?	Gender				
	Male		Female		Total
Yes	89	56%	55	34%	134
No	23	15%	34	21%	57
I do not know about this/ No idea	46	29%	73	45%	119
Grand Total	**158**	**100%**	**162**	**100%**	**320**

The table display that there 56% of male and 34% of female have knowledge about two-factor authentication whereas 29% of male and 45% of female does not have any idea about two-factor authentication service.

iii. Table no. 3

3. Do you aware that victims of fraud and cybercrime should report it to action fraud?	No. of respondent	
I was aware & I have used the services	99	31%
I was aware & I have not used the services	178	56%

No, I was not aware.	43	13%

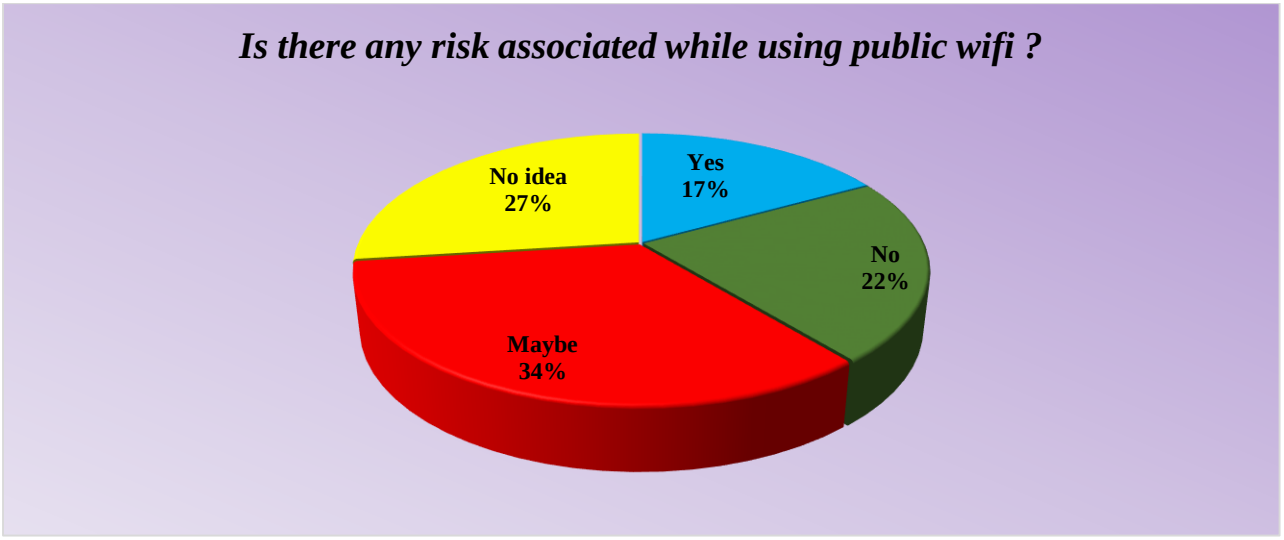
The table indicates that 56% (178) of respondents are aware of the action fraud but they have not used the services while 13% (43) of respondents are not yet aware.

iv. Table no. 4

4. Do you know that you can report a suspicious text message by forwarding it to 7726?	**No. of Respondent**	
I was aware but I haven't used the service.	67	21%
I was aware, & I have used the service.	31	10%
No, I was not aware.	222	69%
Grand Total	**320**	**100%**

The above table represents that 69% of the respondents are not aware reporting of a suspicious message while 10% of respondents know about this and used the service.

Table no. 5 Is there any risk associated while using public Wi-Fi? About 50% of the respondents feels no risk while using public wi-fi or no idea about the threat coming through public Wi-Fi to their device.



VIII. Results & Findings

This study is based on analysis of data collected from 320 sample respondent and the findings is based on this.

1. Majority of the respondent are coming from student group and according to them they spend most of the time for educational purpose on digital platform.
2. Highest number of respondents are (66%) graduate and post graduates. About 58% respondents were from Z generation 21-28 age group.

3. Most of them (54%) spend about 2- 5 hours in a day on various types of digital platforms.
4. Most influencing factors to be digitalized are Time and cost saving, easy availability as it is convenience to all, and our null hypothesis get accepted as Paperless/ Environment friendly is not responsible for the adoption of digital platform as much as others factors influence.
5. Maximum of the respondents (53 %) feels confident about the security of personal devices and online accounts where 25% feels neutral and only 7 -8 % was feeling unconfident.
6. Near 40% respondents strongly agreed that existing laws can control cybercrime, whereas 25% are disagreed and 35% feels neutral about this statement.
7. The study founds that the awareness among majority of respondents towards the security measures while using internet and the two-factor authentication is not up to the mark.
8. Some respondents have knowledge about cybercrime reporting system but they did not use the services.

IX. Suggestions

There are several steps that a person should be aware of for the prevention and control of cybercrime by law and the public in order to prevent cybercrimes:

1. International Standards for security measures must be developed.
2. Internet users should utilise their own methods of communication, such as secret and confidential fibre techniques, and should remove and destroy any confidential information they have used.
3. The operating system must be updated, the antivirus software must be updated frequently, and the password must be changed.
4. Investigating committees and authorities must have the power to deface terrorist websites and networks in order to stop and control online warfare.
5. Appropriate rules and legislation must be adopted in order to prevent and control cyberterrorism.
6. Personal information should never be shared while communicating over multiple social media sites or emails.
7. As a preventative measure against fraud, a person should never provide their debit/credit card information to any phony, fraudulent, or hazardous website.
8. Since it is becoming more and more common for people to utilise photographs of themselves inappropriately, the best course of action is to refrain from sharing any photos or images with online strangers.

X. Conclusion

“Cybercrime is the way to jail; cyber security is way to avail”. The cybercrime in India is growing exponentially. Intellectual property infringement, cyber stalking, cyber extortion, and sexual harassment are just a few of the crimes committed in cyberspace that have been examined in this paper along with the existing statute in the context of Indian law. It is derived from the study that as much as we are getting digitalised the threat of cyber fraud increased parallelly. The government and legislature may spread awareness programme in the form of campaign, advertisements in newspapers, theatre halls, televisions, and

radio etc. Through legal awareness campaigns, the population should be given the necessary knowledge to enable them to protect themselves against the hazards of cybercrime. The time has come for the Indian legal system to catch up with the rise of cybercrimes and the international jurisprudence surrounds them because in the information age, opportunities will emerge for those who are most adapt at utilizing both technology and information.

XI. Bibliography

1. 12-top-cybersecurity-threats-against-organisations-2019-statistics-e1556643214683.jpg (980×585). (n.d.). Retrieved 16 October 2022, from https://cdn.comparitech.com/wp-content/uploads/2019/04/12-top-cybersecurity-threats-against-organisations-2019-statistics-e1556643214683.jpg

2. Crime in India Table Contents | National Crime Records Bureau. (n.d.). Retrieved 16 October 2022, from https://ncrb.gov.in/en/crime-in-india-table-addtional-table-and-chapter-contents?page=27

3. Cyber crime awareness Survey. (n.d.). Retrieved 16 October 2022, from https://www.surveymonkey.com/r/WJGH7MH

4. Cyber Crimes In India. (2022, February). Data Story: Cyber Crimes In India—GS SCORE. Retrieved 4 November 2022, from https://iasscore.in/data-story/cyber-crimes-in-india

5. Digital India Scheme. (n.d.). Retrieved 5 November 2022, from Scripbox website: https://scripbox.com/saving-schemes/digital-india-scheme/

6. Dr. Giridhari Mohanta, Dr. Sathya Swaroop Debasish, & Dr. Sudipta Kishore Nanda. (2017). A Study on Growth and Prospect of Digital India Campaign. Saudi Journal of Business and Management Studies, 02(07), 727–731. https://doi.org/10.21276/sjbms

7. Esther Ramdinmawii, Seema Ghisingh, & Usha Mary Sharma. (2014). (PDF) A Study on the Cyber—Crime and Cyber Criminals: A Global Problem. International Journal of Web Technology, 03, 172–179. Retrieved from https://www.researchgate.net/publication/307594049_A_Study_on_the_Cyber_-_Crime_and_Cyber_Criminals_A_Global_Problem

8. Khan, S. A. (2020). Cyber Crime in India: An Empirical Study. International Journal of Scientific & Engineering Research, 11(5), 5.

9. Megha Solanki. (2022). Awareness of Privacy and Security Concerns using Electronic Devices: An Empirical Study. International Journal of Law Management & Humanities, 5(5), 1038–1058. https://doij.org/10.10000/IJLMH.113686

10. Ravishankar Ulle, Kotresh Patil, Dr Aparna, Dr Niraj Kumar, & Renuka Murthy. (2018). The Impact of Labour Welfare Measures on Employee Satisfaction A Study At Go-Go International Private Limited, Hassan. Journal of Emerging Technologies and Innovative Research, 5(8), 853–857.

11. Sandhya Keelery, & Text, S. C. D. M. up-to-D. D. T. R. in the. (2021, March 10). Cyber crime in India. Retrieved 5 November 2022, from Statista website: https://www.statista.com/topics/5054/cyber-crime-in-india/?

12. SREEDEV KRISHNAKUMAR. (n.d.). Cyber crimes in India rise 6% a year in 2021, Telangana tops list: NCRB data. Retrieved 16 October 2022, from Moneycontrol website: https://www.moneycontrol.com/news/india/cyber-crimes-in-india-rise-6-a-year-in-2021-telangana-tops-list-ncrb-data-9115161.html

13. Tanushree Basuroy. (2022, October 14). India: Number of cyber crimes related to sexual harassment 2021 | Statista. Retrieved 5 November 2022, from https://www.statista.com/statistics/875912/india-number-of-cyber-crimes-related-to-sexual-harassment/

14. Top Cybersecurity Threats in 2022. (n.d.). Retrieved 16 October 2022, from https://onlinedegrees.sandiego.edu/top-cyber-security-threats/

15. Vision and Vision Areas. (n.d.). Retrieved 5 November 2022, from Scripbox website: https://www.digitalindia.gov.in/content/vision-and-vision-areas