WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Study of Awareness About Cyber Laws for Indian Youth

S. Abdul Khadhar, J. Arun

B.A.LL.B. (HONS), Saveetha School of Law, Saveetha Institute of Medical and Technical Sciences

ABSTRACT-

Cybercrime also known as Computer crime, it means any crime that includes a PC and an organisation. As people and organisations increment their dependence on innovation, they are presented to the developing cybercrime dangers. Absence of mindfulness in our youth on such issues would wind up in an extreme harm on monetary, enthusiastic, moral, or moral grounds. Utilising the PCs for our everyday exchanges is very normal nowadays. For instance, we pay our life coverage premium, power charges, save flight or train or transport tickets, request book or some other item web based utilising PC, advanced mobile phones, public perusing communities and so forth. The perpetrating cybercrime are likewise developing step by step with the expanded number of clients doing on the web exchanges. Cybercrime covers a wide scope of various assaults like Cyber blackmail, Cyber fighting, spreading Computer infections or Malware, Internet extortion, Spamming, Phishing, checking (misrepresentation), youngster erotic entertainment and licensed innovation privileges infringement and so on Due to expanded digital assaults nowadays, the internet based clients should know about this sort of assaults and need to alerts while doing on the web exchanges. In this unique circumstance, this paper will survey the development of cybercrimes in India and measures taken by the public authority of India to battle the cybercrimes. The Aim of the study is to analyse these cyber crimes and the measures taken by the public authorities to control these crimes. Totally 200 samples were collected and the SPSS used here is a convenient sampling method.

Keywords: Crime, cyber laws, spamming, security, youngsters.

INTRODUCTION:

The usage of the Internet has turned into a day by day schedule for a larger part of individuals for everyday exchanges. With the expanding web infiltration, protecting the netizens from the developing digital dangers is the difficult errand that a framework should deal with. In India, cybercrimes develop 12% every year . The most recent report of the National Crime Records Bureau (NCRB) showed that the quantity of digital wrongdoing cases has expanded every year and the violations are carried out for monetary profit. Furthermore, there is a winning analysis that Indian digital laws are yet to be prepared and refreshed while contrasting other nation laws. It isn't only the innovation of the Internet that is tricking the clients, however the assembly of the Internet with different stages and administrations that make the clients snare it more than ever. The new measurable data on cell phone web infiltration in India most of the populace got to the web from their cell phone.

Absence of mindfulness on such issues would wind up in an extreme harm on monetary, enthusiastic, moral, or moral grounds. Under such a desperate situation, other than handling the cybercrimes, another issue that should be centred around higher needs is making mindfulness on "cybercrimes and security" among the web clients. The **Aim** of the study is to analyse these cyber crimes and the measures taken by the public authorities to control these crimes. Totally 200 samples were collected and the SPSS used here is a convenient sampling method. The findings of the research clearly reveals that people mostly rely upon web gave data regularly either to office tasks, web based business, banking, business bargains, wellness tips, share markets, and breathe easy action, Consequently it is no distortion to say that advanced cells and other web empowered individual electronic devices have entered each domain of life and opened entryways for cybercrimes to flood in.

OBJECTIVES :

- To study about the design and framework to uphold the awareness programmes among internet users to curb cyber crimes and cyber security.
- To analyse the working of Information technology act 2000 on the prevention of cyber crimes.
- To examine the level of awareness among internet users regarding cyber crimes.
- To find out the various types of cyber crime.
- To evaluate and review the jurisdictional issues on cyberspace.

REVIEW OF LITERATURE :

Malaysia, 1997 The authors in their paper conducted a research in Tricity on cybercrime awareness and revealed that awareness can be increased by giving due importance to cybercrime which can be an efficient tool to decrease or prevent the cybercrimes. They also concluded that it remains the responsibility of the net users as well as the government to ensure a safe, secure, andtrustworthy computing environment.**(Malaysia, 1997)**

Narayan and Thakur, 2000 The author conducted a survey to study the awareness about cyber laws in Indian society .He found that there is a significant difference between the awareness level of male and female users of internet services. The male netizens are more aware of cyber laws as compared to women users. The author in her paper discussed the types of cyber-crime and the cyber laws made to deal with it. Her objective was to analyse whether the internet users are aware of cyber-crimes. She also insisted that it is the duty of all the internet users to be aware of cyber-crimes and cyber laws.**(Narayan and Thakur, 2000)**

Halder and Jaishankar, 2016 Conducted a survey to analyse the cybercrime awareness in Malaysia and found that female students are more aware of cybercrime as compared to male students.The author conducted a survey on 100 respondents to analyse whether netizens are really aware of cyber-crimes. They found to be respondents are somewhat aware of the cyber-crimes,cyber security but still there is an need to be increase awareness among them. Also, they suggested a conceptual model explaining how to uphold and implement the awareness programmes among internet users regarding cybercrimes.**(Halder and Jaishankar, 2016)**

Patil, 2021 There is no doubt that the technology of ICT is growing dramatically with cybercrime. This growth brings an lot of the changes and an revolutions from that traditional methods to electronic means. The change includes government and business and other activity from paper based to be an digital. Also introduced an new methods of bank and other financial transactions under an electronic systems. The impact of digital technology is going very fast and causes a number of challenges. This is why a lot of study written which is based on cyberspace takes part in legal and technique.**(Patil, 2021)**

Brenner, 2010 Alkaabi, Ali Obaid under the study of Combating Computer Crime: An International Perspective examined the approaches used for combating computer crime in Australia, UAE, UK and USA. These four countries represent a spectrum of economic development and culture. He said that the global nature of the Internet has resulted in enormously increased opportunities for cyber criminals. **(Brenner, 2010)**

Khurana and Choiden, 2020 It is also important to identify and adopt best approaches for combating computer crime. He concludes that, is required to continue research into the extent to which legislation, international initiatives, policy and procedures, and technology to combat and investigate computer crime are consistent globally and can be improved upon.**(Arora, Khurana and Choiden, 2020)**

Lim, 2007 However, the Author looks at what approaches to combat computer and cybercrime in developed Countries but the challenges also meet to developing countries like Zanzibar as a part of the United Republic of Tanzania. The threat flows around society since the number of computer users increases every day. Zanzibar identifies the cyber problem and initiates steps to take care of that problem by making amendments to her laws and establishing ICT policy as a running tool to prepare legislation to combat cybercrime. My study will analyse legal documents that applied to stop cybercrime in Zanzibar.**(Lim, 2007)**

Deep, 2018 Ozeren, Suleyman in his study Global response to cyberterrorism and cybercrime: A matrix for International cooperation and vulnerability assessment, he describe that 10Cyber terrorism and cybercrime present new challenges for law enforcement and policy makers. Due to its transnational nature, a real and sound response to such a threat requires international cooperation involving participation of all concerned parties in the international community.**(Deep, 2018)**

Mishra, 2020b The study response to Zanzibar which requires the support from Regional and International cooperation to prevent cyber crisis. Zanzibar has a high risk of cybercrime due to lack of legal measures and cooperation at the international level. The Orezen study will help the Zanzibar to classify cyber terrorism and to frame legal according to the classification.**(Mishra, 2020b)**

Mishra, 2020b According to Nyamaka, Daudi in the study of Electronic contract in Tanzania: An appraisal of the legal framework found that firstly, the globe ecommerce transactions are increasing annually and unless an country creates the requisite enabling legal environment in an time it will miss an opportunities which electronic commerce avails to participants in the globe market. Secondly, since the internet has become a channel of doing business, belated legal responses will create uncertainty and expose participants to unnecessary risks. **(Mishra, 2020b)**

Halder and Jaishankar, 2016 His further recommendation that Parliament and executive agencies with power to enact laws and rules should be able to effect the changes in time because definite articulation of a legal position through a written code is a more preferable approach.**(Halder and Jaishankar, 2016)**

Malaysia, 1997 In study of Electronic Transactions and The Law of Evidence in Tanzania it was found that, as ICT development necessitated changes in the way business transactions are currently conducted, the important challenge posed by the developments, in turn, is the necessity of parallel changes in an both national, international legal framework to accommodate the changes. For an legislative process, there are two approaches are recommended. The first is to enact a comprehensive piece of legislation on ICT and electronic evidence to provide for admissibility of electronic records and documents as well as electronic signatures.**(Malaysia, 1997)**

Nappinai, 2017 The second approach is judicial response. It is recommended that judges should continue to play a pivotal role in extending the existing principles governing paper- based documents and authentication to cover documents and signatures in electronic form. It is recommended that the judges should categorically hold that evidence in a computer hard disk flash disk; compact disk or floppy disk is relevant and admissible to prove or disprove a fact in issue in legal proceedings.**(Nappinai, 2017)**

Brenner, 2010 The two studies above from Nyamaka and with combination research of Mollel and Zakayo 100 percent represent the situation of Zanzibar although the study was written to focus on Tanzania Mainland. Since we are the same country, we also have the same challenges. This study will look after the hard work of the Zanzibar Government to make cyberspace free from crimes.**(Brenner, 2010)**

Mishra, 2020a Rashid Seif Suleiman in his message when introduce ICT policy said that "The Revolution Government of Zanzibar recognises the pivotal role of an ICT sector towards the sustainable socio economic development; equally important is an that ICT enabled development toZanzibar should be policy led, ensuring an better synergy between the public and an private sectors and be an alignment with the national goals. This is the first time that a comprehensive ICT Policy has been elaborated to realise the vision of making Zanzibar a Knowledge based society. This policy document brings together the economic, social and political dimensions of our initiatives in the area of information and communication Technologies.**(Mishra, 2020a)**

Mishra, 2020c "It was noted that there are some clauses that recognize the usage of electronic means in normal human life within Zanzibar legislation; however there is a lack of consolidated and dedicated laws that foresee and promote the usage and the development of ICT in our daily lives; be it personally or officially. On the other hand; there is no authorised institution mandated to oversee overall ICT initiatives within the public sector".**(Mishra, 2020c)**

Higgins, 2009 Mambi, Adam in his book ICT Law Book; he said Tanzania has been slowly shifting her legal system to cope with globalisation, economic and political reform. The development and innovation of technology that brought in the application of ICT around the world caused a great impact to Tanzania. Generally the legal system in Tanzania is mainly based on common law principles. Regulatory steps to secure electronic transactions such as digital signatures, reforms to business laws, dispute settlement and others have not yet been promulgated.**(Higgins, 2009)**

Lim, 2007 His overview about E-commerce and its legal implications at global level is Technology revolution was bringing great changes which are affecting the way business is done. Also the way in which goods and several marketing orders, and ways on which contracts are made and satisfied. This trend addresses great challenges for the offline current laws in Tanzania and other countries which must respond immediately to the developments on electronic transactions for high levels which boost the economy.**(Lim, 2007)**

Halder and Jaishankar, 2016 Mambi explains that the new style of electronic money transfer systems between financial institutions within or outside the country obviously is not clear that is reflected by the legal framework that regulates financial transactions. For instance, the traditional method requirements of writing and manuscript signature which are not acceptable under electronic commerce. These are common features under such laws regulating and governing such business, But under digital technology the requirement of writing and signature is different to our current laws.In addition, he clarifies about the issue of legal implications of electronic security through electronic banking. **(Halder and Jaishankar, 2016)**

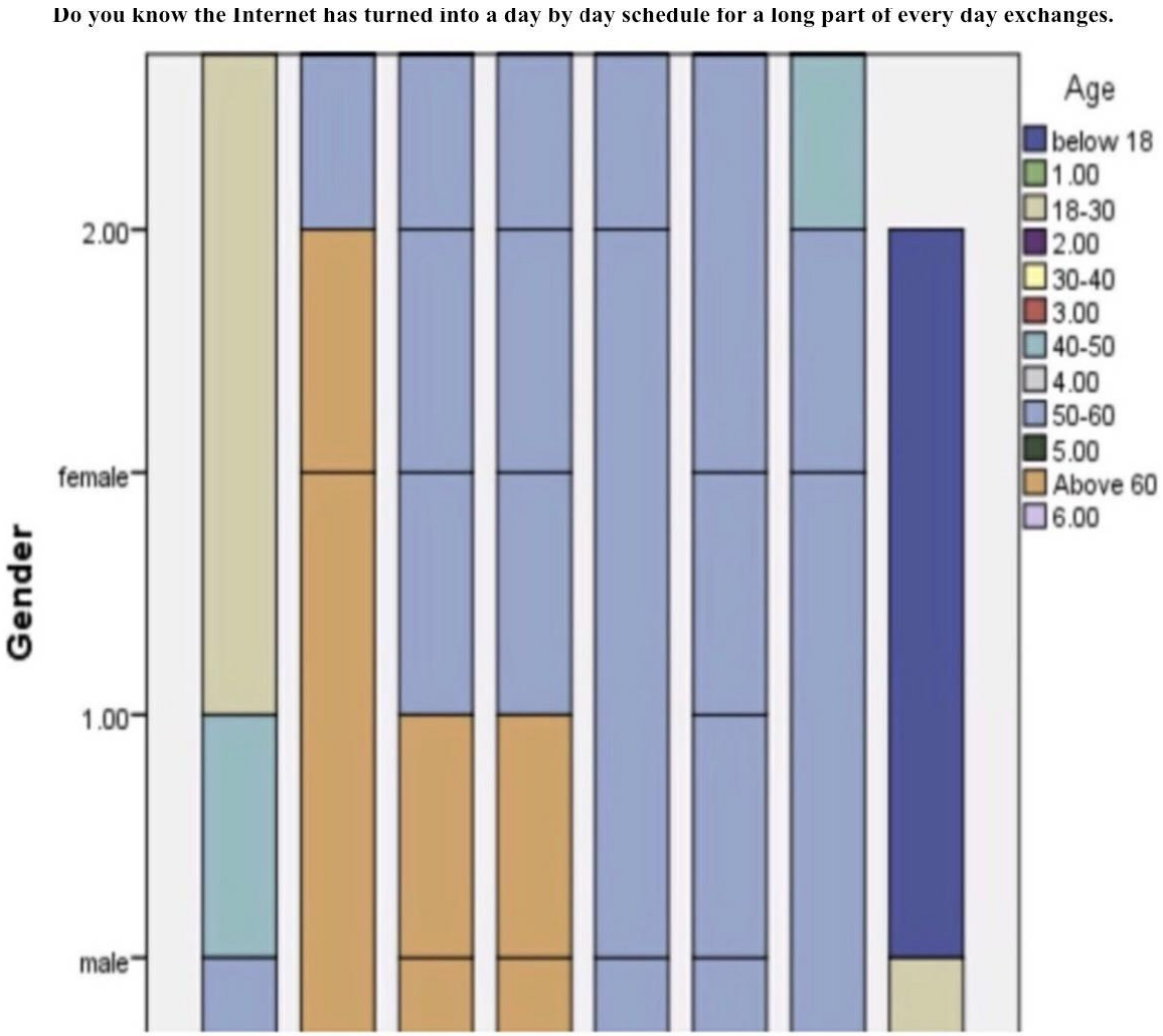
Mishra 2020 The author describes that electronic banking in terms of legal issues is not addressed effectively through policies and legal framework of Tanzania. The current legislation in financial and other related business looks to be not suitable for electronic transactions. The laws that regulate negotiable instruments and Banking in Tanzania do not accommodate online transactions or payments of cyberspace rather than offline transactions.**(Mishra 2020)**

METHODOLOGY :

For the purpose of this study Empirical research is used. It is a way of gaining knowledge by means of direct and indirect observation or experience. This empirical study includes a self tested questionnaire which contains yes or no questions and other choices accordingly by using the survey sampling method. The sample is 200. This is a non- doctrinal study. This paper depends on both primary and secondary data. The primary data for the present study is collected using sampling techniques. Random sampling is used to collect the primary information from the respondents. A random sample selected from the parliamentary form of government and presidential form of government. The primary data which has been analysed using Frequencies, Chi-Square test and Crosstab method, Anova. The secondary data is collected from books, journals, articles and e-sources. The researcher has also utilised books, articles, notes, comments and other writings to incorporate the various views of the multitude of jurists, with the intention of presenting a holistic view. The dependent variables are age and Occupation.

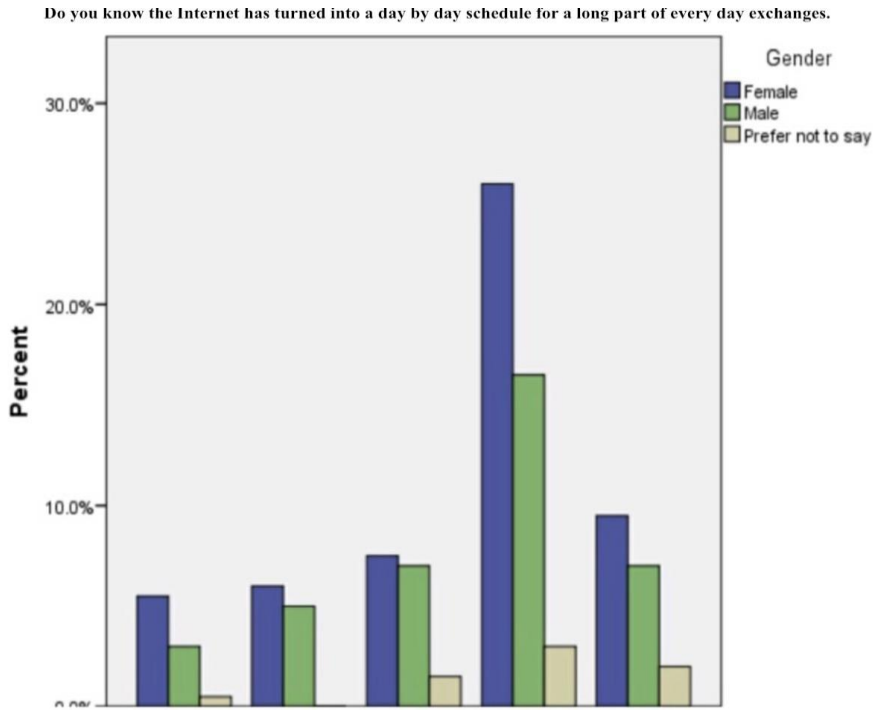
ANALYSIS AND DISCUSSION :

CHART : 1



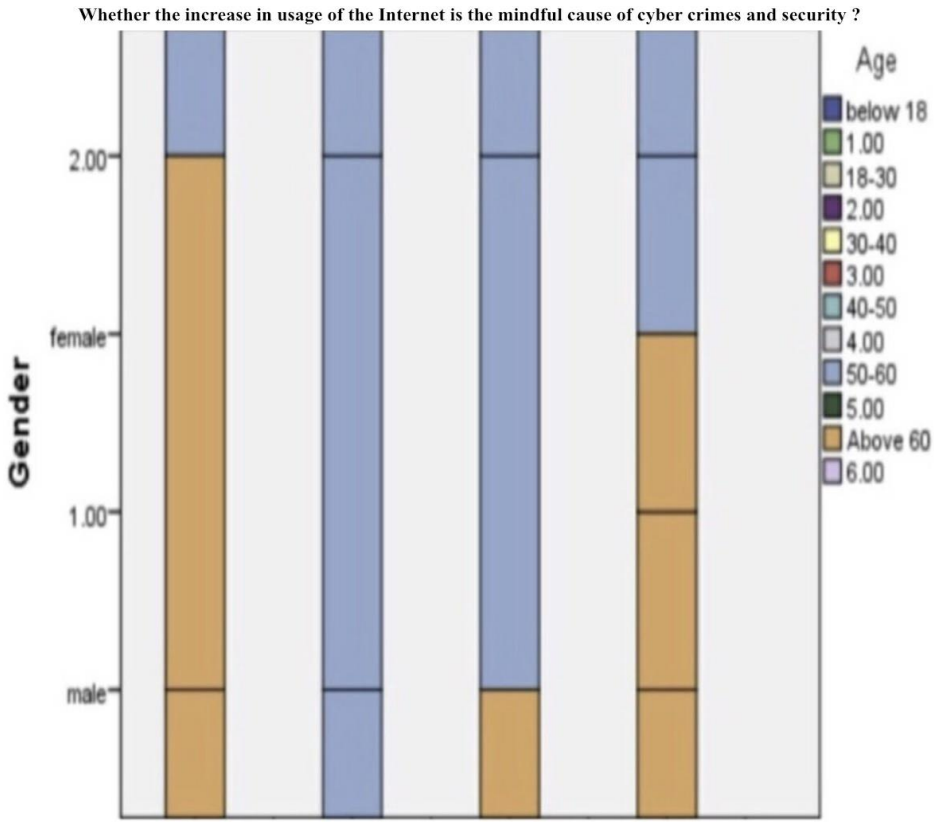
LEGEND : Majority of the respondents are between occupational groups 18-30 years and the least number of respondents are between the age of Above 60 years.The chart shows the Age of the respondents who answered the question most people answered yes and it was accordingly mentioned in the graph.

CHART : 2



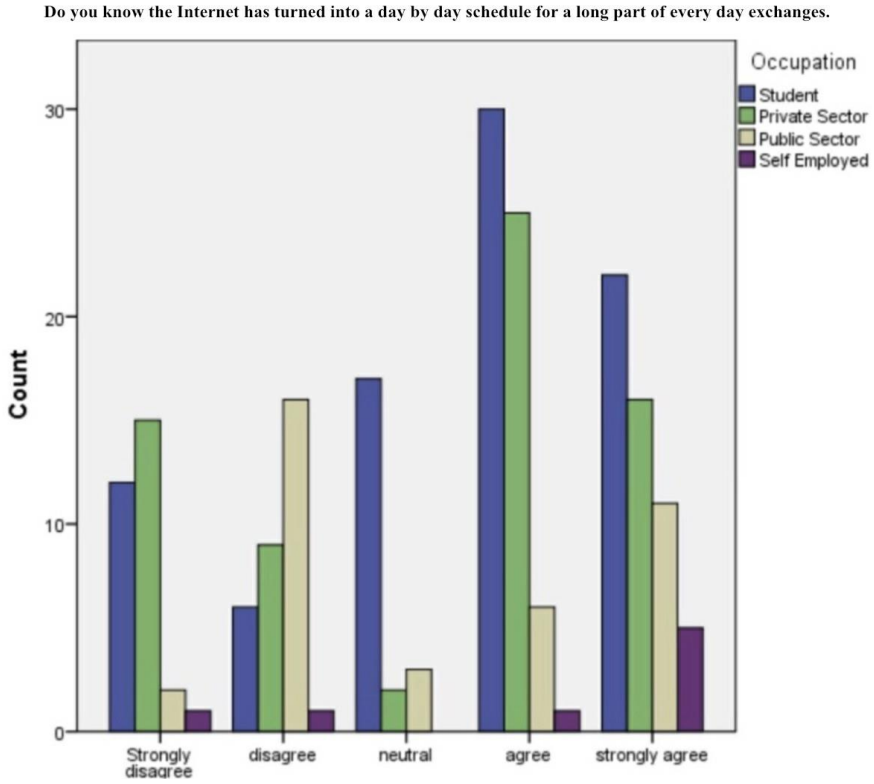
LEGEND : Majority of the respondents are female and the male respondents are comparatively less according to the bar diagram shown.

CHART : 3



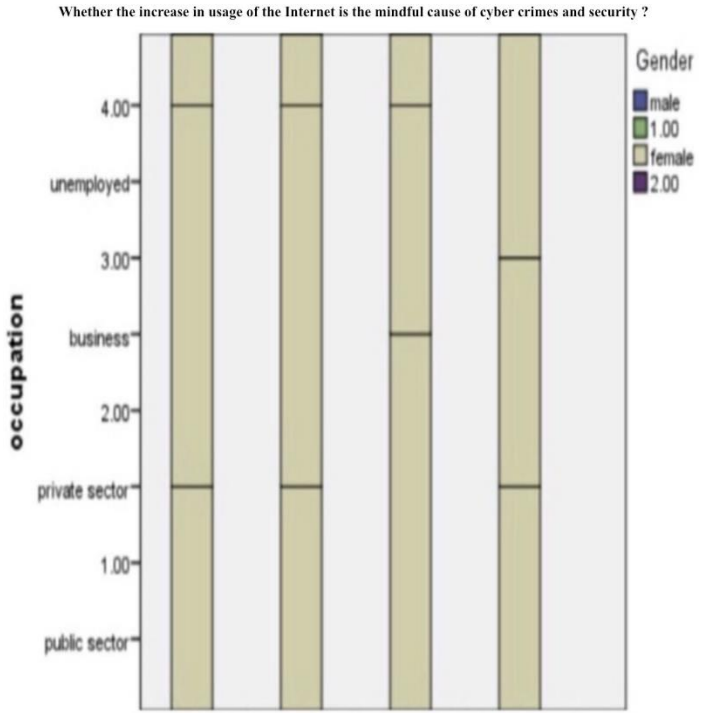
LEGEND : Majority of the respondents are between occupational groups 18-30 Years and the highest number of Respondents are between the ages of Above 60 years.

CHART : 4



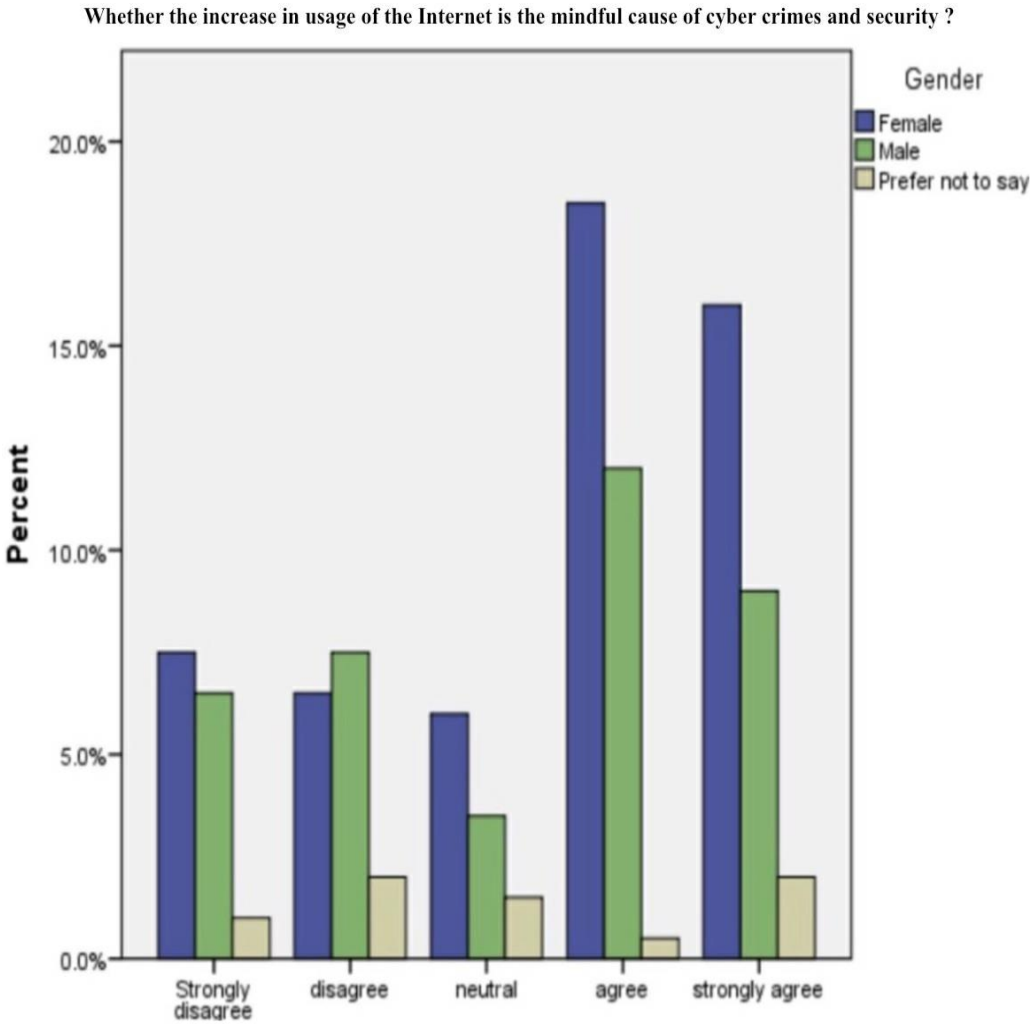
LEGEND : Majority of the respondents are Students the independent variable is compared with the dependent that is the occupation and the bar diagram was drawn accordingly.

CHART :5



LEGEND : This graph is compared with both the independent variables such as Gender and Occupation which the respondents answer, this shows the majority of male who are unemployed.

CHART : 6



LEGEND : This graph comparatively shows the percentage of the respondents along with the dependent variable and classified accordingly.

RESULTS :

CHART : 1 The people below the age of 30 are not aware of the question asked but the people between 30-50 mostly answered properly because people below 30 are not involved in electronic matters and avoid the habit of reading newspapers and articles related to electronic and cyber crimes and its prevention activities which are happening in our daily life.

CHART : 2 The chart shows the Gender of the respondents who answered the question most people answered yes and it was accordingly mentioned in the graph, the male responders are not aware of the question asked but the female responders mostly answered properly according to their will.

CHART : 3 The chart shows the gender and Age of the respondents who answered the question most people answered yes and it was accordingly mentioned in the graph, the people below the age of 30 are not aware of the question asked but the people between 30-50 mostly answered properly according to their will.

CHART : 4 The chart shows the gender and Occupational status of the respondents who answered the question most people answered yes and it was accordingly mentioned in the graph, the people who are unemployed are not aware of the question asked but the people who work in the public sector mostly answered properly according to their will.

CHART : 5 The chart shows the gender and Age of the respondents who answered the question most people answered yes and it was accordingly mentioned in the graph, the private sector people not aware of the question asked but the people unemployed are involving in daily matters and avoids the habit of reading news papers and articles related to the modern and the technological and development activities in the country.

CHART : 6 The chart shows the gender of the respondents who answered the question most people answered yes and it was accordingly mentioned in the graph. The females are aware of the question asked but the people who choose Prefer not to say are mostly answered properly according to their will.

DISCUSSIONS :

CHART : 1 The responses as per the above shown chart, for the question 1; Does the federal government have the most power in our country ? respondents are between occupational groups 18-30 years of age and the least number of respondents are between the age of Above 60 years.

CHART : 2 Majority of the respondents are between occupational groups 18-30 Years and the least number of Respondents are between compared with their age groups.

CHART : 3 Majority of the respondents are between occupational groups above 18-30 Years and the least number of Respondents are between the ages of Above 50-60 years.The chart describes the responses collected for the 2nd question.

CHART : 4 The respondents are classified between occupational groups 30-40 Years and the least number of Respondents are between the ages of Above 60 years.Here the occupation and age of respondents are mentioned accordingly in the chart.

CHART : 5 Majority of the respondents are between occupational groups of 18-30 Years and the least number of Respondents are between the ages above 60 years.

CHART : 6 Majority of the respondents are between occupational groups above 18-30 Years and the least number of Respondents are between the ages of Above 50-60 years.The chart describes the responses collected.

LIMITATIONS :

The major limitation of the study is the sample frame The major amount of respondents were connected through different social platforms. So the online surveys didn't help in interactive collection of responses. There were audiences who were not aware of the concept of privatisation and few Respondents were not aware about the usage of online sources. So a larger audience was not reached. The restrictive area of sample size is also another drawback.The physical factors are the most impactful and a major drawback to the research. The researcher had to face time restraints on college campuses. Survey question options may lead to clear data because certain answer options may be interpreted differently by the respondents.

CONCLUSION :

Criminal misconduct on the Internet, or digital wrongdoing, presents as one of the Major difficulties of things to come to India and International law authorization. New abilities, innovations and analytical methods, applied in a worldwide setting, will be needed to recognize, forestall and react to cybercrime. This new business will be portrayed by new types of wrongdoing, a far more extensive degree and size of culpable and exploitation, the need to react in a significantly more convenient manner, and testing specialised and legitimate intricacies. Imaginative reactions, for example, the formation of cybercops, cyber courts and cyber judges may ultimately be needed to conquer the critical jurisdictional issues. Computer crimes portrays an extremely general classification of offences. Some of them are as old as PC offences, like theft or misrepresentation, then again, actually a PC or the Internet is utilised in the commission of the wrongdoing. Others, such as hacking, are remarkably identified with PCs. The public authority should ensure the security of the state computerised network and frameworks which store significant public data and should make substantial strides during this respect. The lockdown has uncovered the feeble digital laws and after several 5 percent expansion in digital wrongdoings, the govt. has moved some concentration to the current side and furthermore the digital focuses and digital police became dynamic. The govt. is giving a warning to the overall population to not succumb to those main wrongdoings and play it safe while filling their subtleties and passwords on web-based destinations. Be that as it may, the govt additionally should think of some more grounded laws, systems, and strategies to get the programmers. Plus, there's a need to acquire some security applications to thwart the organisations' frameworks and emergency clinic PCs from hacking. These are some of the momentary arrangements during the lockdown yet there likewise needs some change inside the current Information Technology Act, 2000 on the grounds that it very well may be a far reaching act and does exclude a large part of the contrary angles which are covered with the digital violations.

REFERENCES :

1. Arora, M., Khurana, P. and Choiden, S. (2020) *Performance Management: Happiness and Keeping Pace with Technology*. CRC Press.
2. Brenner, S. W. (2010) *Cybercrime: Criminal Threats from Cyberspace*. ABC-CLIO.
3. Deep, M. K. (2018) *Cybercrime and Ethics among Kids and Teens. Study on top four countries in Cybercrime*. GRIN Verlag.
4. Halder, D. and Jaishankar, K. (2016) *Cyber Crimes against Women in India*. SAGE Publications India.
5. Higgins, G. (2009) *Cybercrime: An Introduction to an Emerging Phenomenon*. McGraw-Hill Humanities/Social Sciences/Languages.
6. Lim, Y. F. (2007) *Cyberspace Law: Commentaries and Materials*. Oxford University Press, USA.
7. Malaysia (1997) *Cyber Laws*.
8. Mishra, A. K. (2020a) *An Overview on Cybercrime & Security, Volume - I*. Notion Press.
9. Mishra, A. K. (2020b) *Cyber Laws in India - Fathoming Your Lawful Perplex*. Notion Press.

10. Mishra, A. K. (2020c) *Intellectual Property Rights in Cyberspace*. Notion Press.
11. Nappinai, N. S. (2017) *Technology Laws Decoded*.
12. Narayan, A. and Thakur, L. K. (2000) *Internet Marketing: E-commerce and Cyber Laws*.
13. Patil, S. (2021) *Securing India in the Cyber Era*. Taylor & Francis.
14. Malaysia (1997) *Cyber Laws*.
15. Mishra, A. K. (2020a) *An Overview on Cybercrime & Security, Volume - I*. Notion Press.
16. Mishra, A. K. (2020b) *Cyber Laws in India - Fathoming Your Lawful Perplex*. Notion Press.
17. Mishra, A. K. (2020c) *Intellectual Property Rights in Cyberspace*. Notion Press.
18. Nappinai, N. S. (2017) *Technology Laws Decoded*.
19. Narayan, A. and Thakur, L. K. (2000) *Internet Marketing: E-commerce and Cyber Laws*.
20. Patil, S. (2021) *Securing India in the Cyber Era*. Taylor & Francis.