Asian Journal of Organic & Medicinal Chemistry **ISSN Online: 2456-8937**
Vol. 7 No. 1 (January - March, Special Issue - III 2022) **UGC CARE APPROVED JOURNAL**

Understanding Cyber Safety and Security With Respect to SocialMedia

Nikita Tipnis, Purva Sawant and Anand Hindolia
PTVA's Institute of Management, India

ABSTRACT
This paper mainly focuses on the concepts of cybercrimes, social networking sites and the victims. The problems of cybercrime have been discussed in detail and the paper tries to providethe best possible solution to the problem. We have used a quantitative method of analysis to study the awareness of cybercrime. Today's world is facing a common issue of cyber-attacks on social media, especially by the teens. They are unknowingly becoming the victim of cybercrime.

Keywords : Cyber safety, Cyber security, Social media, Cyber-attacks, Online stalking, Cyberbullying, Sexting, Privacy concern, Digital footprints, Cyber investigating cells, cyberpolice, Cyber lawyers.

1. INTRODUCTION

"We're all going to have to change how we think about data protection."Chris Van Daele (2017)

"Privacy – like eating and breathing – is one of life's basic requirements." Katherine Neville (1992), (A Calculated Risk: A Novel)

"If you put a key under the mat for the cops, a burglar can find it, too. Criminals are using everytechnology tool at their disposal to hack into people's accounts. If they know there's a key hidden somewhere, they won't stop until they find it."

Tim Cook (2015), One of the favourite platforms of communication of today's generation is social media. It isused for receiving and sending information, entertainment and to connect with people.

The Social community group is known as social media such as Instagram, Facebook, Twitterand many others. It is the number one choice among the children. Although this media is very useful it has some cons. Lack of cyber security is the biggest cons of social media. So it is the responsibility of the parents to see to it that there is no misuse of their children's information. Even the information can be used for cyberbullying. As teenagers spend most of their time in chatting with their friends on social media, there is a rising risk of cyberbullying, cyber fraud, sexting, online harassment, etc.

The children face many other problems such as depression, sleep deprivation, anxiety, etc. However, on the other part, the parents find it difficult to cope up with technology and the digitalmedia. They are unaware of the digital world which is there inside social media. This results in a lack of connection between children and their parents. Hackers take this situation as an advantageand it leads to cybercrimes.

Social media addiction has been a serious issue which has been faced by children and adolescents. Many of them are also been exposed to contents which are viral and inappropriate atthe same time.

Threat to youngsters from social media Adolescents are being trapped by hackers as they are unaware of the fact that their footprintsare being traceable.

1. Online stalking

Online stalking is one of the most common threat to social media users. The stalker stalks the profile, their data, photos and other personal information through online mode. They can be easily traced the online footprints of the user with the help of advanced technology and this hampers the privacy of the user's data.

2. Cyberbullying

Cyberbullying is a form of online harassment where the user's data is stolen for personaland unethical gain. Most of the adolescents are prone to this type of threat. When it comes to online harassment, it is less risky as compared to physical harassment.

3. Sexting

Sexting is considered as highest form of threat especially to young girls. The victim also to suffer from mental trauma. The sexually banned messages, nude photos and semi- nude photos are being sent or received. The adolescents who are being part of this, has to face serious consequences under cyber and IT laws.

4. Privacy concern – Digital Footprint

Since the youngsters are unaware of the fact that their data may be misused, they donot pay attention to privacy issues. Their each and every activity on social media is been traced and thus it is known as the **'Digital Footprint'**. Privacy hazard is a major concern for adolescents.

Apart from these cyber threats, there are several other threats to adolescents with respect to social media. To Overcome this threats, government has introduced the need for the security requirements.

Crimes that take place online through electronic devices are known as cybercrime. It is mostly a virtual crime. It affect individual mentally, emotionally, psychologically and economically. It is also done to spoil one's name in the society through online mode. Cybercrime includes harassment, stalking and spread of sexual context. It violates laws which are made to regulate internet based activities

Cyber law is formed to look after the regulation of information technology. It is concernedwith legal aspect of data in online form. It is concerned with privacy of data, protection of privacy and misuse of data, security of data, circulation of information, etc.

Cyber laws are protecting people by preventing cyberbullying which takes place in inter- gender as well as in all age demographics. To enforce cyber laws that deal with cybercrimes, the information technology act was passed by the Indian parliament on **17th October 2000**. It was signed by the then Minister of Information Technology**, 'Pramod Mahajan'**. Many amendments were made after the act in cyber laws. Punishable actions were imposed on offensive messages, child porn and cyber terrorism.

To create a healthy environment on social media we must spread awareness in order to secureour online data. To trace cybercriminals, there are many cybercrimes investigation cells and cybercrime police stations. These cells are situated in various parts of the country. A victim of cybercrime can register or file their complaint. There are many cybercrime complaints filed with respect to social media. The number of social media cybercrimes are increasing day by day in India.

Also the concept of cyber lawyer is becoming more and more popular. They are cyber professionals who helps people in taking care of their data online as per the cyber laws. Even many companies have started taking help of cyber lawyers to prevent their data from cybercrime.

2. LITERATURE REVIEW

Li and Berno (2008) state that it is necessary to know how relationships are developed in social media. Technology has evolved but its influence on personal interactions has been moreprofound.

Rajagopal (2013) claims that consumers are becoming more engaged in co-creating marketing material with companies and brands. As a result, businesses are looking at virtual social media programmes and campaigns to better reach their customers who live online as well. The creation of social media method on YouTube, Facebook and Twitter looks separate event rather than being a segment of a non – segregated advertising process.

Hanna et al (2011) also discuss with this development and say that the buyers aren't anymore passive within the selling exchange technique. He believes that some firms produce social media platforms and operate it severally, not as associate integrated strategy that brings consumer's experiences first. Social media doesn't replace conventional media, however it will enlarge marketing's capacity to have interaction with customers and acquire consideration and influence.

F. B. Schneider (2013) displayed a paper on the need for legitimate implementation of cyber security instruction in educative institutions or colleges. He expressed that the necessity of cyber security instruction in colleges advance expansion of non-formal ponder centres in cyber securityformation. The deficiency of well-trained labour in cyber security makes the work of cybercriminals simple. They encourage submitted that there was the requirement for standardized preparation of cyber security experts such/ that they get all the desired preparation to empower them to protect against cyber dangers. The gadgets utilized by an individual that are associated with the web are troublesome to hacking the event that h/e/she has essential knowledge of cyber security. So, cyber security is preparing moreover diminishes the number ofcyberattacks episodes to form the work of cybercriminals more difficult.

3. OBJECTIVES OF RESEARCH

The Review of Literature was conducted to study the following objectives:-

- To understand about Cyber Safety in India.
- To check the knowledge level of Cyber Safety in India.
- To suggest the security measures to social media users.

4. RESEARCH METHODOLGY

4.1 DATA COLLECTION

The study is based upon primary data collected from 100 respondents through a structured questionnaire covering different group of peoples of different age groups engaged in various types of occupation. The secondary data has been collected through various research papers and from information available on web links.

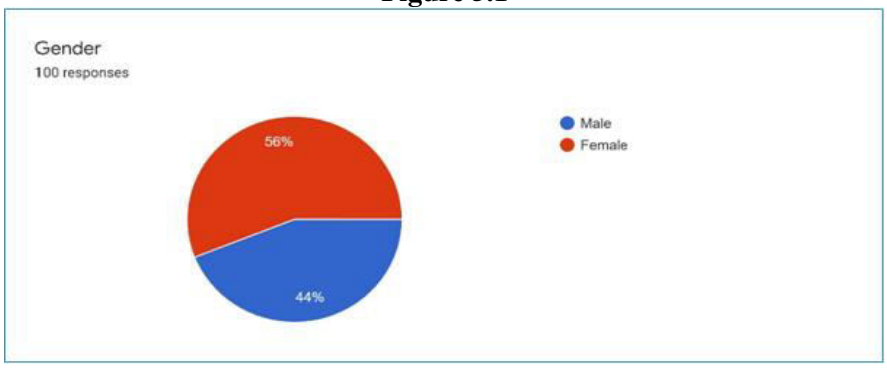
4.2 DATA ANALYSIS

Analysis of data was done with the help of Questionnaire. The percentage analysis method wasused for finding out the results of the survey.

5. ANALYSIS AND INTERPRETATION

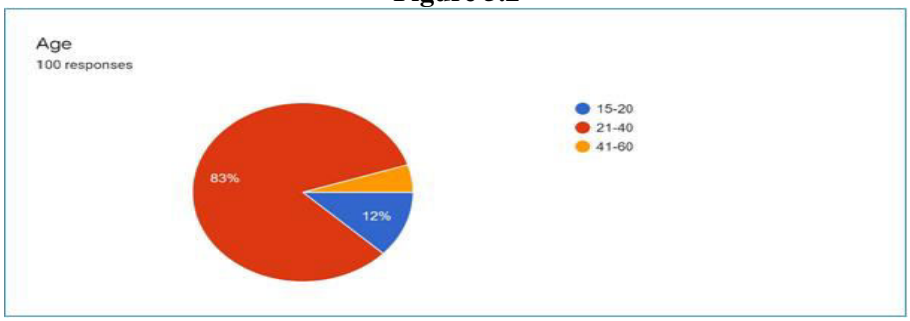
The analysis and the interpretation of the survey are as follows:

Figure 5.1



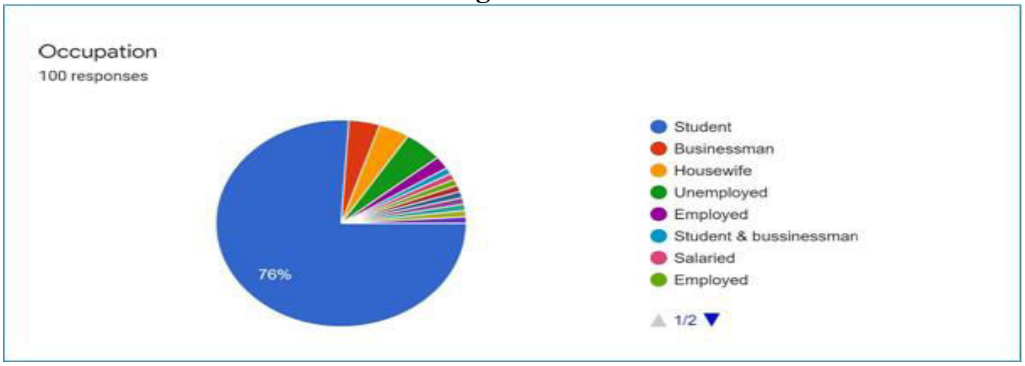
According to the pie chart (5.1), 56% are male and the remaining 44% are females.

Figure 5.2



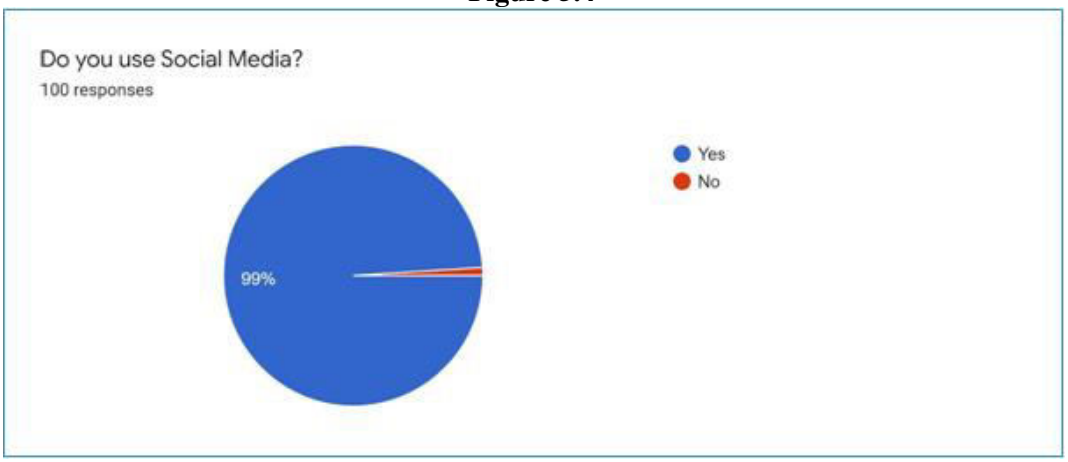
According to the pie chart (5.2), there are three different categories of age, of which highest responses are received from categories 21-40 that is 81.3% followed by 15-20 age group that is 12% and the least being from the category of 41-60

Figure 5.3



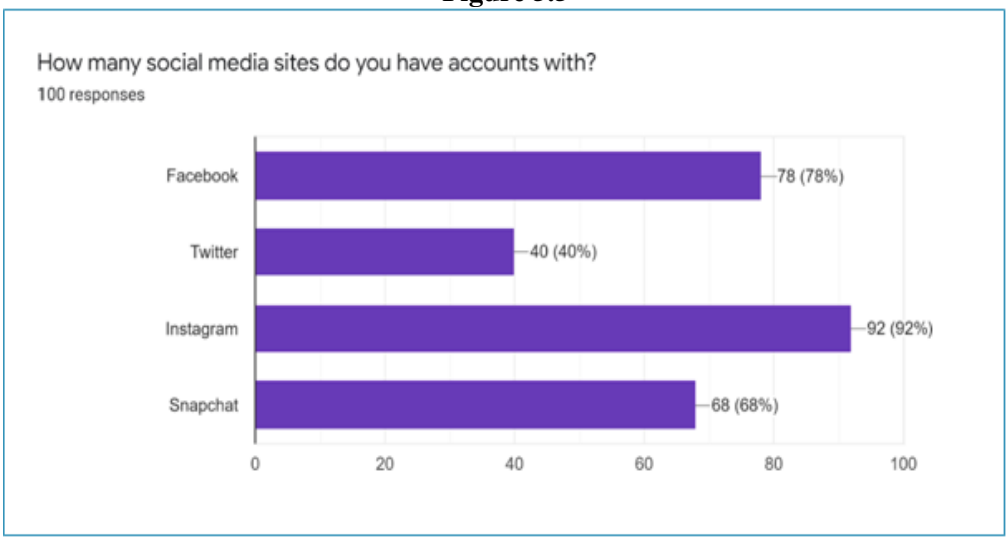
According to the pie diagram, the majority of the respondents are from the category of students and the remaining respondents are from various other categories such as employed, unemployed, self-employed and housewife.

Figure 5.4



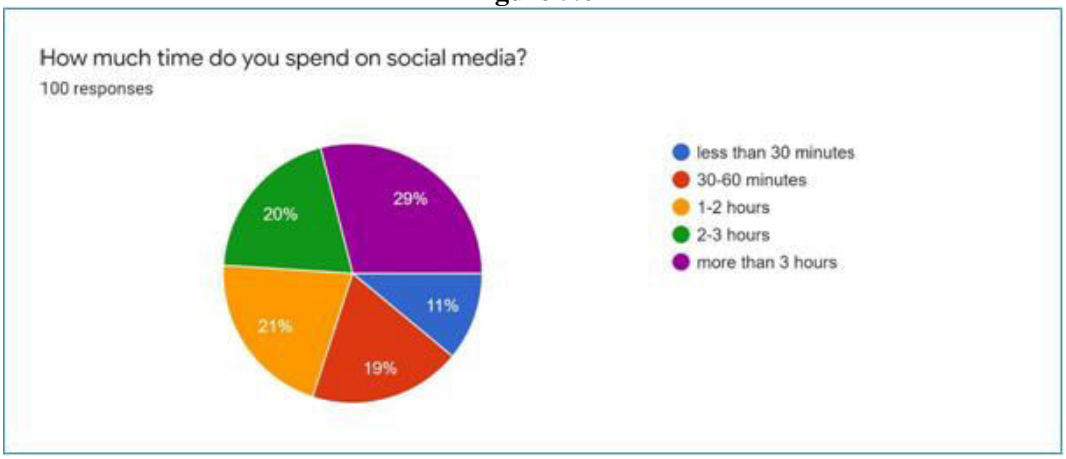
According to the survey, 99% of respondents use social media that who don't use social media is1%

Figure 5.5



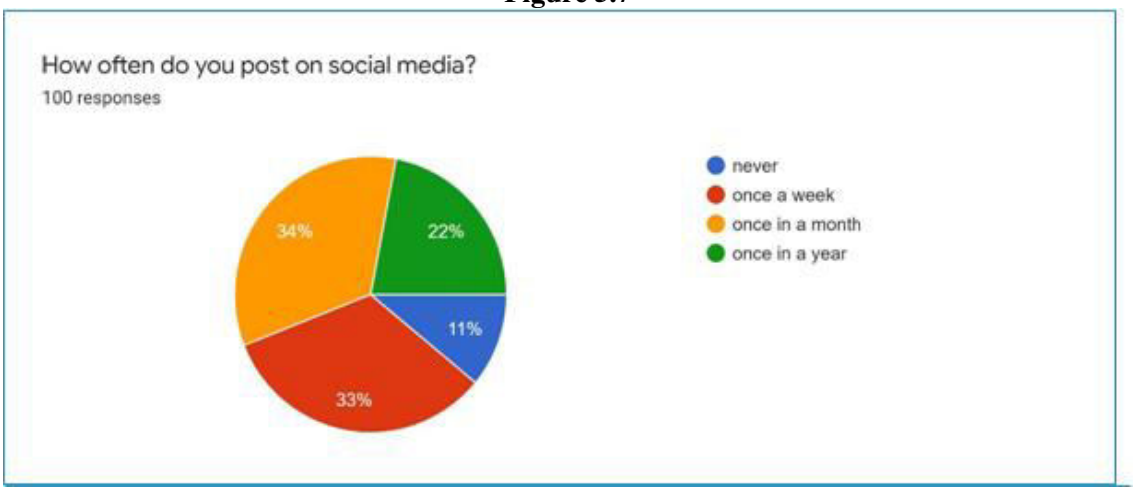
The pie diagram represents that the respondents addicted more to Instagram is 78% followed by Facebook 78%, twitter 40% and snap chat 68%

Figure 5.6



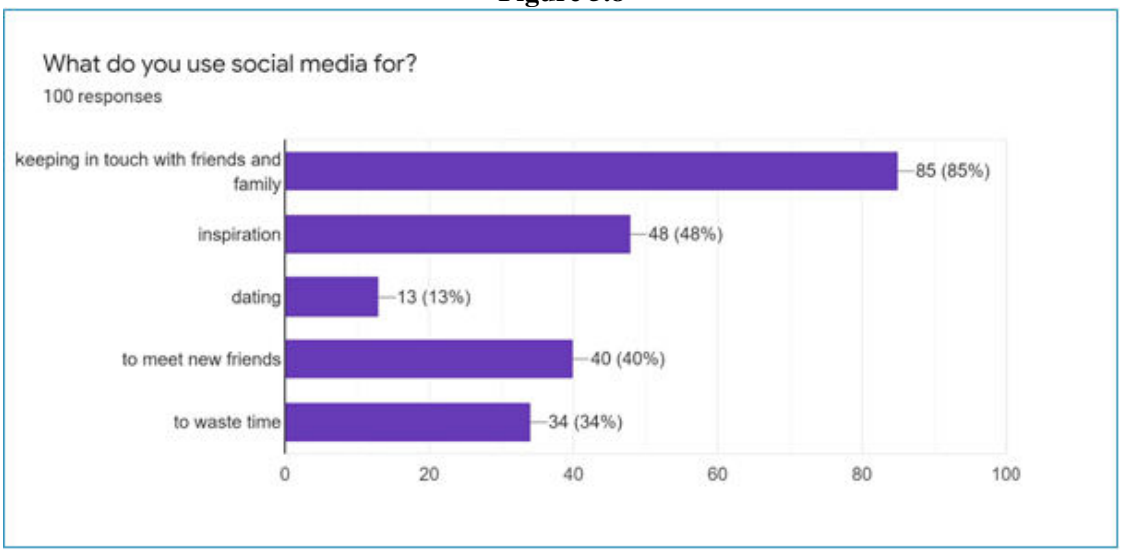
The pie diagram, states that the maximum amount of time spend by the respondents is more than3 hours 29%, 1-2 hours is 21%, 2-3 hours is 20% 30-60 minutes is 19% and less than 30 minutes is 11%

Figure 5.7



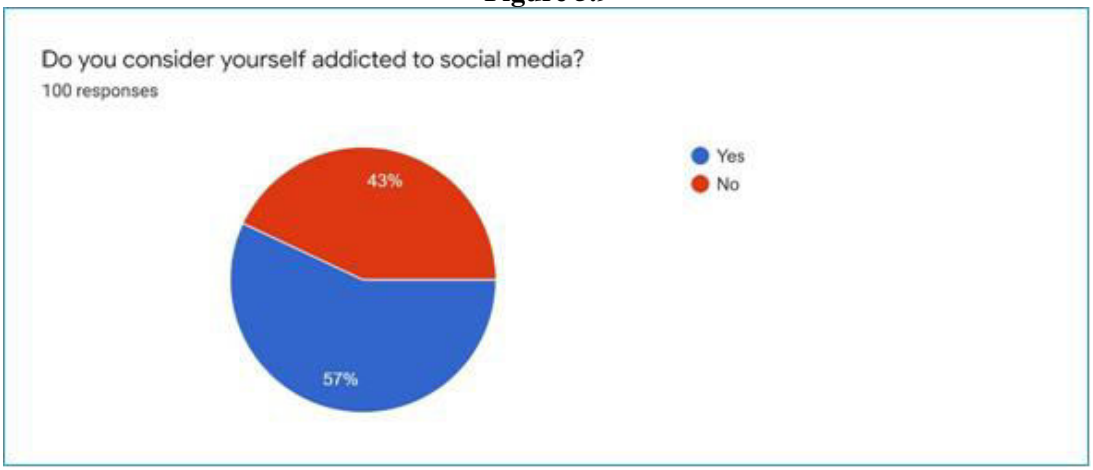
The above pie diagram represents that the frequency of posts posted by the respondents once aweek is 33%, once a month is 34%, once a year is 22% and those who never posts is 11%

Figure 5.8



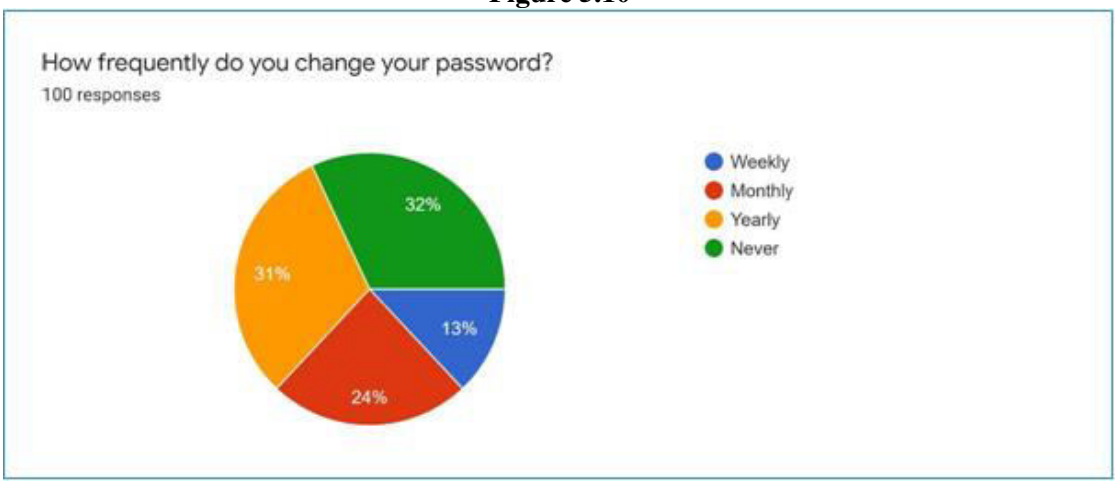
The pie diagram indicates that the respondents using social media for keeping in touch with their friends and family are 85%, for motivation and inspiration is 48%, dating purpose is 13%, to get introduced with new friends is 40% and for leisure is 34%

Figure 5.9



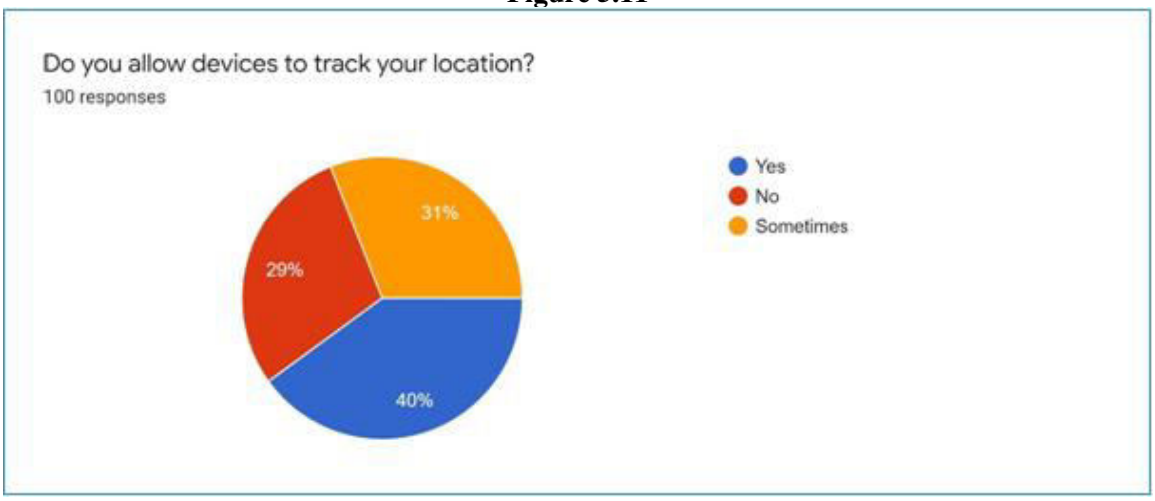
The pie diagram indicates that the number of respondents addicted to social media is mammoth which is 57% and those who are not addicted to social media is very few that is 43%

Figure 5.10



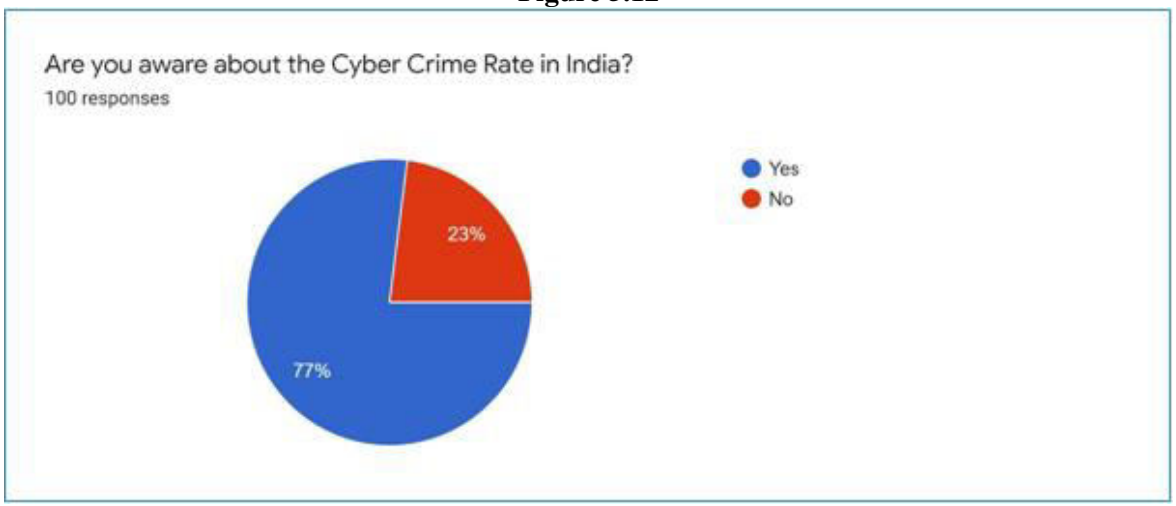
The pie diagram represents the respondents who change their password on weekly basis is 13%, changing on monthly basis is 24%, yearly basis is 31% and those who never change their passwordor try to avoid changing their password is 32%

Figure 5.11



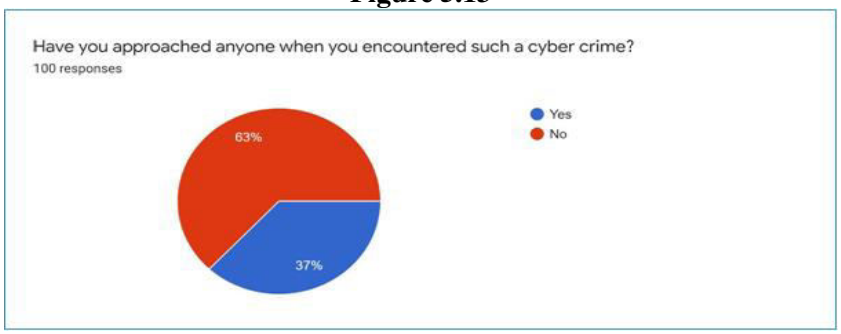
The above diagram states that the respondents allowing the devices to track their location is 40% The respondents not allowing the devices to track the location is 29% and the respondents which allows the devices to track the location depending upon the situation is 31%

Figure 5.12



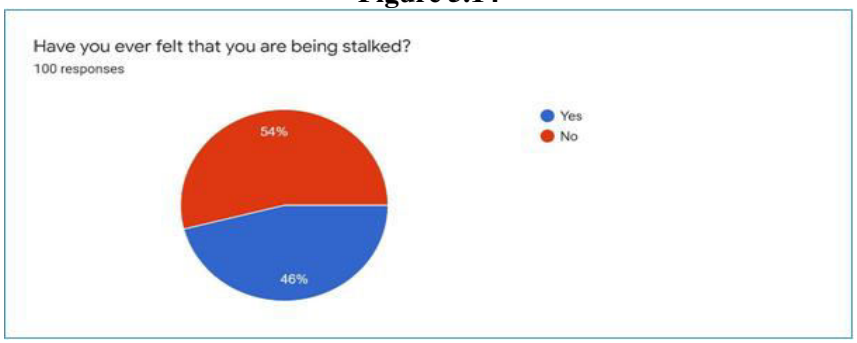
The above diagram indicates the no. of awareness among the respondents is quite favourable whichis 77% and very few are not aware that is 23%

Figure 5.13



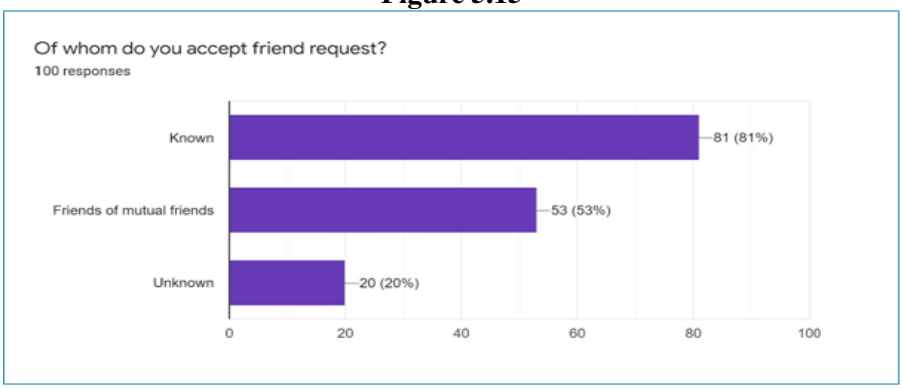
The above pie diagram states that the respondents approaching the grievance cell or any other respective body is very low 63% and the respondents approaching is 37%

Figure 5.14



The above diagram indicates that the respondents that have being stalked are less as compared tothe respondents who are not stalked.

Figure 5.15



The above pie chart, shows that the respondents that tends to accept the friend requests of their friends, family and relatives are high which 81% The respondents accepting friend requests fromunknown people and stranger is 20% which is a good sign as long as the safety is concern.

6. CONCLUSION

There are many people in the society who are becoming the victim of cybercrime in India. There have been many laws introduced by the government of India in order to prevent the cybercrime. A common mode of cyber-attack is from social media and majority of the victims arenone other than children, adolescents and teens.

The research indicates the electronic devices are the major factors which indicates the use of Social Media and its influence on these generation. It can be said that around 1.16million cyber security cases and presently a 3x spike from the past. Talking about the cyber safety in India, the country has been receiving hundreds of planned and executed cyber-attacks. Modern hackers have learned to utilize thousands of different techniques and methods for collecting information and money from various organizations. Any organization that possesses sensitive data is a potential target of cyber-attacks. The primary reason of these cyber-attacks is cyber illiteracy. We were nottaught about how to use internet. Our cyber education started from cyber cafes, where we only learnt how to use sites like Google, Yahoo and Facebook. We were never taught important things like the guidelines to use the internet and digital safety. Many parents overshare pictures of their children online and

destroy their right to privacy which can further lead to embarrassment, bullying and may damage online reputation.

Sometimes not only strangers but also known people build an emotional connection with children and young people online to gain their trust for the purpose of sexual abuse or exploitation. After a point of time when they come to know that they are convinced by their talks they start building sexual intimacy, which then leads to blackmailing, bribing, and threats. This thus can beavoided by protecting personal information for examples not sharing your birth date, address, and phone number on social media or any other online platforms. Make usernames that never uncovergenuine character. Ignore companion requests from cloud people on social media stages. Be alertwhen your chat partner starts complimenting you about your appearance within a short span of time. Do not talk to people who ask for your sexually explicit photos or videos. Learn to block. Talk to your elders or parents if your chat partner suggested to keep your conversations with themsecret. You can also report the same to helpline numbers. Share location to apps for which it is actually required. Also, Facebook policy doesn't allow a child less than 14 years of age to create an account. Surprisingly, Netflix, YouTube and Amazon Prime instructs 'Kids Mode' for all children underneath the age of 14.

To conclude, the cyber security cells, cyber police, government and we as the citizen of India should focus more on educating the young as well as the elder population of the country regardingthe rising risk of cybercrime in India. Also there is a need of spreading the awareness about the prevention measures to be taken and most importantly how to deal with the cybercrime.

7. REFERENCES

1. Jadhav Y.A., Jain S.J., More B.S., Jadhav M.S., Chaudhari B. (2021) Cyber Safety Against Social Media Abusing. In: Singh M., Tyagi V., Gupta P.K., Flusser J., Ören T.,Sonawane V.R. (eds) Advances in Computing and Data Sciences. ICACDS 2021.
2. Communications in Computer and Information Science, vol 1440. Springer, Cham. https://doi.org/10.1007/978-3-030-81462-5_12
3. Gwenn Schurgin O'Keeffe, Kathleen Clarke-Pearson, *Pediatrics* (2011) 127 (4): 800–804, (The impact of social media on children, adolescents and families), (The American academy of paediatrics) (https://doi.org/10.1542/peds.2011-0054)
4. Pavitra Prakash Singh, Vijay Kumar, Dr.Majid Sadeeq (2019) (Cyber Bullying as an Outcome of Social Media Usage: A Literature Review)
5. Sabina Matook, Brain Batler (2014), (The International Encyclopaedia of Digital Communication and Society), DOI:10.1002/9781118767771.wbiedcs097
6. Allen H. Moffitt (2022), (American journal of orthodontics and dentofacial orthopaedics, official publication of the American Association of Orthodontists, its constituent societies, andthe American Board of Orthodontics, 161(3):477.e1-477.e2, DOI:10.1016/j.ajodo.2022.01.
7. Hanna, Richard; ROHM, Andrew; Crittenden, Victoria L. (2011), (We're all connected:The power of the social media ecosystem.) Business Horizons, v. 54, n. 3, p. 265–273, maio 2011. Disponível em: <http://linkinghub.elsevier.com/retrieve/ pii/S0007681311000243>. Acesso em: 9 mar. 2012
8. Fred B. Schneider (2013), (Cyber Security Education in Universities), (IEEEspEdtrl.July2013)
9. Chris Van Daele (2017), (https://www.linkedin.com/pulse/were-all-going-have-change-how-we-think-data-privacy-chris-van-daele), (https://www.finestquotes.com/quote-id-29328.htm), (https://www.linkedin.com/pulse/were-all-going-have-change-how-we-think-data-protection- sean-evers)
10. Katherine Neville (2002), (https://www.goodreads.com/quotes/433504-privacy---like-eating-and-breathing---is-one-of)
11. Tim Cook (2015), (https://techcrunch.com/2015/06/02/apples-tim-cook-delivers-blistering- speech-on-encryption-privacy/#.bicc3p:8KJ4), (https://cooltechzone.com/news/microsoft-warns-of- newly-detected-nobelium-malware)
12. Daniel B. Chorney, Michael F. Detweiler, Tracy L. Morris, Brett R. Kuhn, P (2008), (The Interplay of Sleep Disturbance, Anxiety, and Depression in Children, *Journal of Pediatric Psychology)*, (Volume 33, Issue 4, May 2008, Pages 339– 348), (https://doi.org/10.1093/jpepsy/jsm105)