Can Cyber Crime Be Done Through Social Media?

Mr. Rohit Sharma & Mr. Mohit Sharma

ABSTRACT

The basic need of human being is cloth, shelter and food but now a day Internet has also become a basic need of human being. Internet play an important role to connect person to person through social media i.e., new media. Each and Every technology has its own pros and cons and it is paradise for cyber criminals. Social media applications like face book, what's app, Instagram, Twitter, YouTube etc. are new means of media which are available to the variety of audience according to their groups, ages and classes. People can create an account on social media to interact socially with one another and make long lasting relations with them besides this, people play game through different application also. But on the other side it is attack to someone's privacy which can lead to different type of illegal activities by using Internet (social media), such as name, location, and email address. There are many crimes which are done through social media where criminal use the computer technology.

Keywords – Social media, Internet, Cyber-crime.

INTRODUCTION

Cybercrime is a crime involving computer and internet technology (account hacking, extortion, spamming, and child pornography and hate crimes). Cybercriminals can use computer and Internet technology or a hacked account for personal use to access someone's personal information.

Cybercrime is also known as Internet and computer crime. Hacking, exploitation, child pornography, child pornography, cyber terrorism and unauthorized computer access are common types of cybercrime. Serious crimes like cyber terrorism are the biggest cyber crime because it causes havoc across the country.

Crimes that target computer networks or devices include viruses and rejection attacks. The Information Technology Act 2000 was enacted to deal with cybercrime in the use of computer networks, including cyber stalking, phishing, identity theft or fraud. It defines cybercrime and fines them.

Types of Cyber crime

1. Hacking: - When another person enters a computer security system for personal gain. A person who commits such crimes is called a hacker. Now this crime has mostly happened.

2. Child pornography: - Make a video of someone sexually abusing a child, the video he / she posted on the internet is called child pornography.

3. Cyber exploitation: - When someone hacks someone's email server or computer system and asks for money to restore the system, blackmail means cyber exploitation.

4. Cyber terrorism: - Information related to a government agency such as DRDO can be hacked by a criminal known as cyber terrorism, which is prevalent across the country.

Categories of cybercrime

There are three main categories: individual, property and government:

Property: A hacker hacks into a person's bank details to gain access to funds, makes purchases online to give people their information, and demands money to restore the system.

Person: Criminal hack computer security system or establishing emotional contact with children for personal gain Cyber tracking, distribution of pornography, child rearing and trafficking.

Government: Information related to a government agency such as DRDO, also known as cyber terrorism, can be criminally hacked.

Social media usage

Social media is a kind of new medium through which people around the world find and communicate shared ideas such as interests, emotions, feelings and insights. Similar social media application: -

Facebook: - Now the world's most powerful social media application and network, people have started communicating easily with others.

Twitter: - Twitter is a social networking site that is well suited for business and professionalism.

Instagram: - This is a visual platform designed for users to share, comment, post and interact through digital media.

What's app: - It is a messaging app for communicating with each other through text (chats), audio chats and video calls. Other social networking sites missing from the list are Google+, Snapchat, YouTube etc.

OBJECTIVE

1. To know safety about the information among users when they are online.

2. To identify the cyber security is essential to be safe online.

3. To find out the most common crime done through social app.

4. To study the various precautions take by user to prevent cyber crime.

5. To know the need of awareness about cyber crime, cyber security and related laws.

HYPOTHESIS

1. H0 - Users are not feel safe about the information when they are online.

   H1-Users are feel safe about the information when they are online.

2. H0- The cyber security is not essential to be safe online.

   H1- The cyber security is essential to be safe online.

3. H0- There is not any crime done through social app.

   H1 - There is any crime done through social app.

4. H0- User doesn't take any precautions to prevent cyber crime.

   H1- User takes any precautions to prevent cyber crime.

5. H0 – There is no need of awareness about cyber crime, cyber security and related laws.

   H1 – There is need of awareness about cyber crime, cyber security and related laws.

REVIEW OF LITERATURE

A review of literature is a search and an evaluation of the available literature in your given subject or chosen topic area. It is documents the state of the art with the respect to the subject or topic you are writing about. A literature review shows your readers that you have an in depth grasp of your subject, and that you understand where your own research fits into and adds to an existing body of agreed knowledge.

The literature review on crimes which are done by internet or social networking site explain that this new crime spreading quickly around the world. So, it is necessary to ask what are the measures laws related to this type of crime. So, there are many literature of review which is explained the positive impact as well as negative impact of cybercrime.

According to the author **Das and Sahu (2011)** the personal and private life has become unidentifiable. People have become more active on social networking sites, and tends to forget their personal life, and spending more time on internet. Social networking sites have become a privacy threats to our private life. We can simply get someone's details without their consent and that's the exploitation of human basics rights. Criminals and hackers can use it to get access to your personal data, pedophile can lure more victims and social networking sites have the facility and ability to make happy and healthy life, miserable. Hackers can hack through your data and exploit you and have an access to your personal data that could get steal without your consent. The authors haven't given any ways or action to be on the safe on-line.

Welsh (2011) calls today's generation "digital natives" or" I- genesis", it basically a collection of study that's tells the social and as well as psychological effects of continuous networking. High usage of social networking sites have negative effects on health such as lack of fellow feeling, hyperbolic aggression and schizophrenic psychosis and most commonly depression as cause of psychological state. Even though most students uses internet for their betterment and enhancements of their knowledge but studies have proved that social networking keep many adolescents from the learning.

Heyy and morselli (2011) believe that with the recognition of social networking sites, the road gang social group has emerged online. Social networking sites have created a very easy and simple way for everybody, people of same beliefs and thought and opinions to share their knowledge and views.

In another necessary work, **Ahan (2012)** presents a study that believes in the positive aspects of the social networking sites and it shows the bridge and bond of social capital with the adolescence of social networking sites. With the help of social networking sites many people especially adolescent are making the best use of the internet in so many ways, students and working people are fully utilizing the internet and social networking sites for the personal growth and professional development as well. This text suggests that social networking sites should have additional positive effect than negative effects, because the author believes in positive relationship of social networking sites and social capital.

Another author **Mikami (2010)** explain the biological process in the terms of social communication that adolescence may be a time once peers have a bigger impact on personal, social, and activity performance. Throughout this point the standard and amount of peer interaction will increase dramatically. Now-a-days, a vital a part of peer interaction happens on-line for many teenagers. The author presents two arguments on on-line interactions; the first argument emphasizes that on-line interactions area unit worse than offline interactions, and the other hand another argument represents that the internet is a medium of communication which is mostly used by youth as a replacement medium. He aforementioned the standard of relationships was low as results of Internet-based interactions, as nonverbal cues and visual communication weren't out there on-line. He argues that web use contributes to poor adjustment, as a result of on-line social interaction isn't a relative alternative for intimate faces. Another read is that somebody's face characteristic conjointly plays a vital role in on-line media. They noted that adolescents with face-to-face relationships could have folks that use the net as an extra house to of times act for social interaction. Their analysis shows that people who use on-line social communication area unit balanced youth (early and later adolescence). So, the author focuses on its positive aspects of social networking sites and also ignores the negative impacts of social networking sites and internet.

LIMITATION OF STUDY

There are certain limitations which cannot be ignored:-

- The response given by the society may not be accurate.
- This is not quite physical to cover all the area of Delhi – NCR, only few colleges of Delhi from where the data was collected.
- Another limitation of the study is most of the people are not comfortable to talk or even they were not comfortable to give the data because they are not aware about the cybercrime then the answer was not satisfactory for specific point.
- There is not any involvement of any professional of IT department for this study.

SIGNIFICANCE OF STUDY

Cybercrime is a global problem that is engulfing the world in a frightening way and India has not escaped from it. Cybercrime is a unique threat that can be carried out against any computer system and user in the world from anywhere. This is global evil, and is becoming more and more difficult to control. As a result, governments, businesses and individuals around the world are facing serious economic consequences and the new challenge of tackling cybercrime.

Cybercrime mainly affects not only the government but also the citizens; especially cybercrime has been reported to be on the rise in banks and mobile transactions, targeting cybercriminals who have little or no understanding of this technology.

The rise in these crimes raises the big question, why have the legal machines not yet done to deal with this situation. The legal climate in India is still not conducive to cyber security in the country. This is due to the development of laws that preceded the development of computer technology.

Cybercrime is one of the topics in focus at Global Oneness. The importance of this study is to know the various precautions that consumers take to prevent cybercrime, because cyber security is very important in protecting information and data from cybercrime. A lot of people have already done research on this subject, so I want to know some facts and no one has enlightened it.

Every individual and organization is targeted for cybercrime and vigilance is absolutely essential. We know that the Information Technology Act 2000 provides a legal framework for cybercrime and under the law enshrined in the Constitution of India, there is a provision to punish those who commit crimes through the Internet.

Therefore, the purpose of this study is to study the status of cybercrime in relation to previous legal procedures.

RESEARCH METHODOLOGY

For this research, questionnaire as a method of collection of primary data have chosen. The analysis of the primary data would be done through statistical examination represented by graphical representations. Besides questionnaire case study as a method of collection of secondary data have chosen for this research study.

Universe

The target population of this study is Delhi (different district of Delhi) and Delhi NCR People who use internet for communication and interact to each other through different social media network sites broadly means people from all age groups, especially between 17-30 years of age i.e., youth because in this age, people spend more time on social media sites.

Sampling technique

Convenience sampling have used for this research study. Respondents who were conveniently available are selected through convenience sampling. About 1.9 crore of Delhi's population comprises of the youth and adults. The sample results got from 300 respondents who are mostly students and they are response which is based on their availability and willingness to complete the questionnaire.

Data Collection

This research study involved a number of case study and questionnaire. Data was collected from both sources i.e.; Primary source and secondary source. The printed questionnaire paper shared directly to the respondent who is easily available. The questionnaire had a brief description of the project in the beginning.

CASE STUDY

Case 1 - Orkut fake profile cases

As all know about Orkut.com which is a popular online social media platform, where subscriber can communicate with people of common interest and share information, join groups and communities. Because of cyber crime world, various fake or duplicate profiles which contains defamatory information about the victims of sexual harassment, child abuse, immoral behavior that results in people become mental and physical disturbed.

Case 2 - Pune Citibank Emphasis Call Center Fraud

One of the cyber crime fraud is “data protection” has raised a number of concern, as data is very important tool in daily life. There is a case reported in which former employees of the BPO division of MPCS Ltd have defrauded US customers of Citibank worth Rs 1.5 crore. This type of crime was done by gaining unauthorized access to the client’s digital space, and that crime is mentioned under IT act 2000, and punishable. Any IPC offense using electronic documents can be considered an offense using written documents, like, fraud, conspiracy, breach of trust etc. Is applied to the above case also mentioned in ITAct-2000. The offense under ITAct-2000 was sanctioned under Sections 43 and 66. According to the act, persons involved in these types of cyber crimes will be imprisoned and fined, and liability to pay compensation to the victims will be up to a maximum of Rs. 1 crore per victim.

Case 3 - Bank NSP case

The Bank NSP case a type of crime in which fake emails ids is created and further is used to lose many clients. This is occurred when bank management trainees are married, both belong to same bank or organization. The couple exchanged several emails using company computers. After that somehow if they divorced or parted away for a while, the girl or boy created fake email ids like "Indian Bortions" and sent emails to the boy's foreign clients and ultimately, he/she used a bank computer to do so. The company or organization lost many clients. The bank is responsible for emails sent using the banking system, and comes under legal surveillance.

Case 4 - Cyber attack on Cosmos Bank

In August 2018, Cosmos Bank, Pune branch lost Rs 94 crore in a cyber attack. The process is to hack the main server of the bank; the intruders were able to transfer money to another bank in Hong Kong. Firstly, they hacked into the ATM server to get the details of visa cards and rupee debit cards customers. The connection between the switching system, i.e. the centralized system and the payment gateway are attacked, and a security breach is there. According to an international cybercrime case study, a total of 14,000 transactions were made using 450 cards in 28 countries. Nationally, 2,800 transactions were made using 400 cards. It was the first malware attack that shut down all communications between the bank and the payment gateway.

Case 5 - Account Hack

Yashmita Grover, aged 25, is a lifestyle blogger from South Delhi. She has 80,000 followers on the social media app, not long ago. "She said - In May, she received a personal message on Instagram to click on a link to verify an account after then she lost access to account. Later, she contacted the police and wrote e-mails to the police.

Case 6 - Kumar v/s Whitely

In this case, the defendant gained unauthorized access to the Joint Academic Network (Janet), added files, changed passwords, and denied access to authorized users. After investigation which revealed that Kumar was logged in by BSNL broadband internet connection and altered the computer database associated with authorized user, and subscriber broadband Internet user accounts. The Central Bureau of Investigation, India has registered a cyber crime against Kumar and started the investigation based on a complaint lodged by the Press Information Bureau, Chennai which detected illegal use of broadband internet. According to the complaint, the subscribers lost Rs 38,248 due to Kumar's misconduct. He also hacked the websites of Bangalore, Chennai and other cities. Verdict: Additional Chief Metropolitan Magistrate gave NG Arun Kumar Egmore, sentenced to one year rigorous imprisonment under 420 IPC (fraud), Section 66 (computer) offense of IT Act, 2000).

Case 7 - The fake profile of the President was posted by the cheater

On September 9, 2010, the fraudster created a fake profile in the name of Hon'ble Presidential Pratibha Devi Patil. After that he has been arrested in connection with four fake profiles created in the name of the esteemed president on Facebook, a social media website. The fake profile of the president on Facebook is misleading the public. The first information report was registered under sections 669 of the Information Technology Act 2000.

Case 8 - Instagram Account Hack

Rinku Agarwal, 34 years old, owned an online business that supplied niche products. She received multiple orders due to her 2.3 million Instagram followers. Earlier this month, she could not login to his page. 70% of my clients did not know what I was doing or they could not contact me because my Instagram page did not exist.

Case 9 - Sandeep Waghis v/s State of Kerala

A criminal offense has been registered against nine persons under Sections 65, 66, 66A,C and D, filed by a representative of a corporation engaged in the petrochemical trade and distribution business in India and abroad. The company has a website called www.jaypolychem.com in name and style, however, another internet site www.jayplychem.com has been set up. The first accused was Sandeep Varghese (a.k.a Sam), he was fired from the company. Sam sisters and brother-in-law, including other accused in the conspiracy with Preeti and Charanjit Singh.Defamation and malicious cases about corporate and its directors are made available on the website. The accused's sister and brother-in-law were in Cochin and were dealing with known and unknown persons who had collectively defrauded the corporate and two accused Amardeep singh and Rahul were involved in the act of forgery and fraud. In order to defame the name and image of the corporate and its directors, they sent emails from the fake e-mail accounts of many buyers, suppliers, and banks. The defamation campaign of all the above people has done which creates huge damage to the name and the reputation of the corporate. Later the company suffered a loss of crore of rupees from corporate producers, suppliers and customers and was unable to attempt to do business after that

Case 10 - Nehru University MMS Scandal (Punishment for Violation of Privacy)

As many cases of MMS encountered in academic institutions and University is common, so this is also a similar case in which a pornographic MMS clip was made on campus and aired outside the university. Some media reports two accused initially when they tried to extort money from the girl from that video clip, but somehow, they failed, they put the video on mobile phones, on the web and it was sold as a CD in the Black Film market.

NOTE - ***The cases mentioned above associated with cyber crimes in India after analyzing these, it had been found altogether cases that in most cases the account is said to Hacking Issues. According to the level of crime, the criminal was also punished under the Information Technology Act 2000.***

DATA ANALYSIS AND INTERPRETATION

The questionnaire was made with the help of pen & pencil questionnaire and was distributed to college's students and thus the researcher has got responses from 300 respondents.

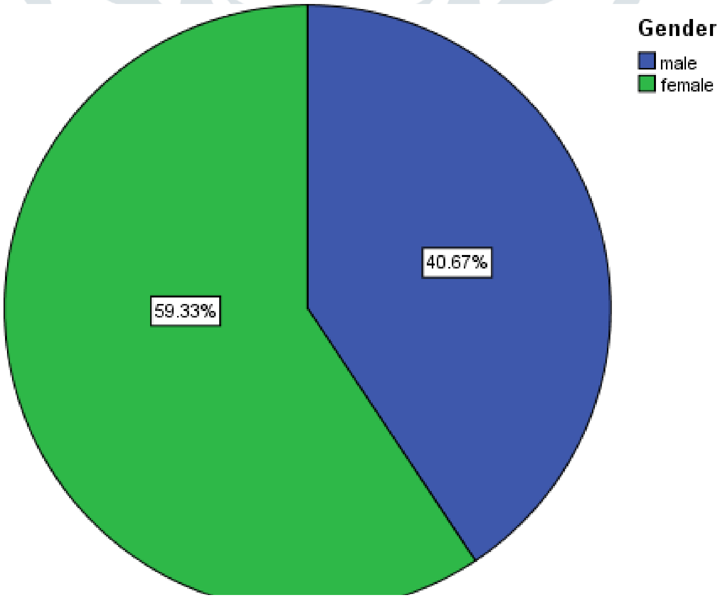

Fig. no. 01

59.33% Respondents are female students and 40.67% respondents are male students.

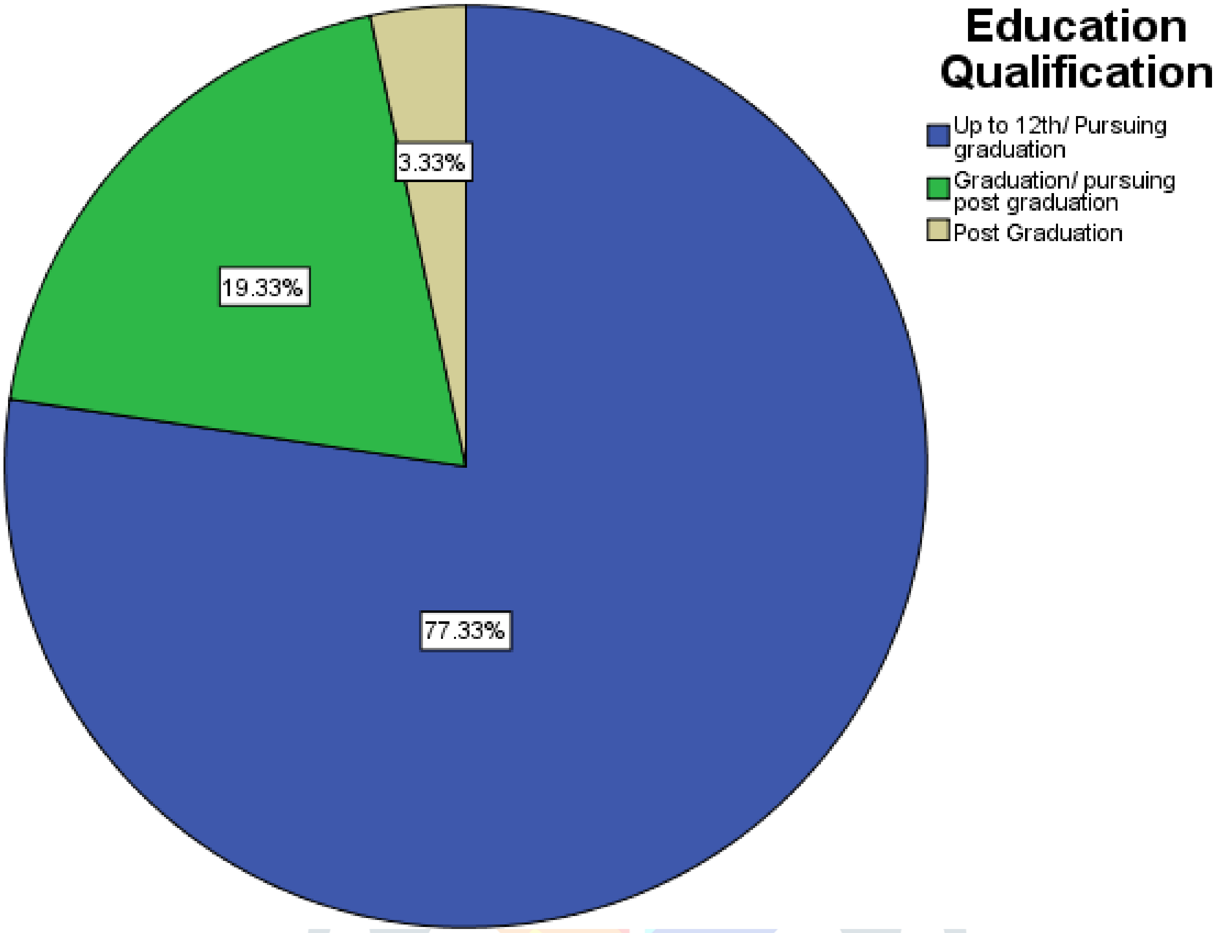

Fig. No. 02

77.33% Respondents are pursuing graduation or passed 12th class, 19.33% respondents have passed graduation or pursuing post graduation and3.33% respondents have passed post graduation.

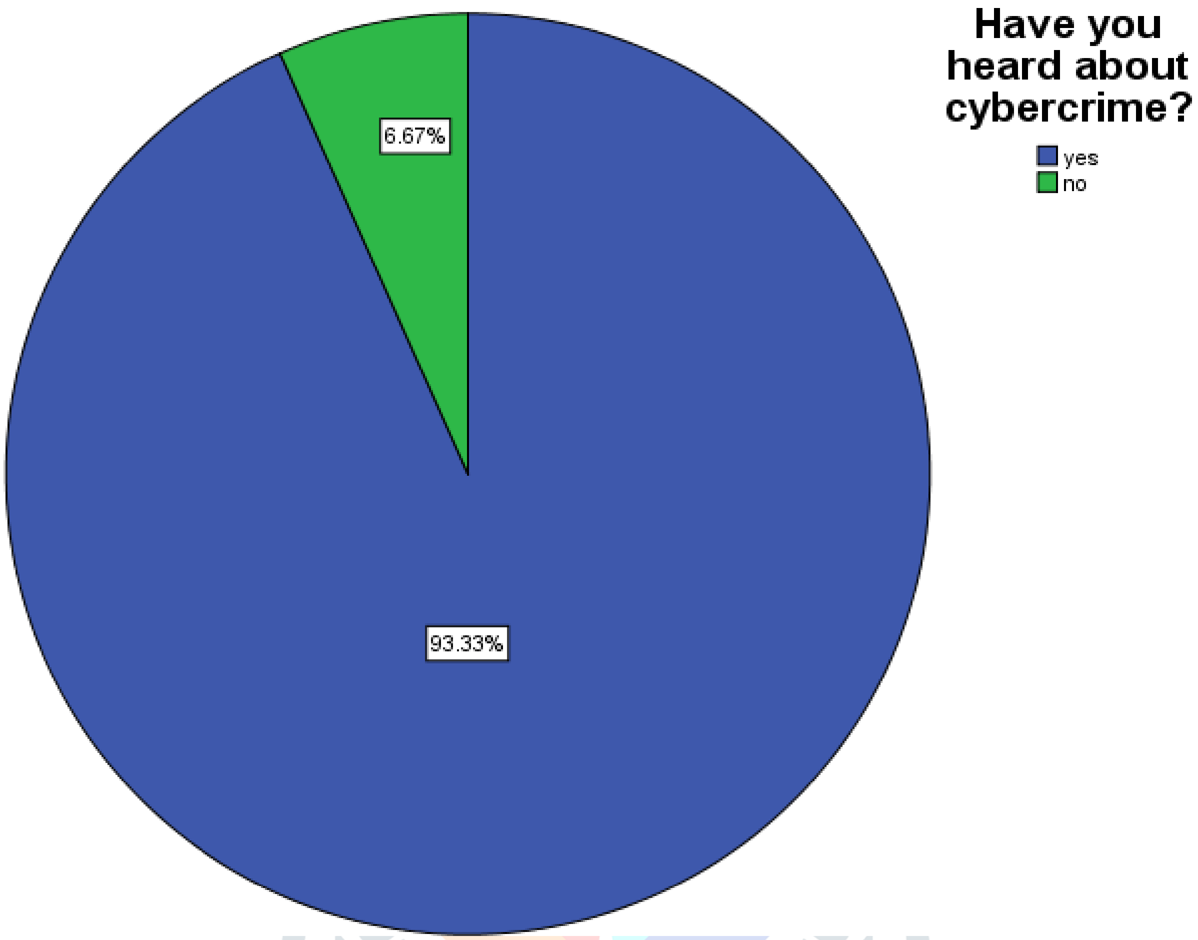

Fig. No. 03

93.33 % respondents have heard about cybercrime but 6.67% respondents not.

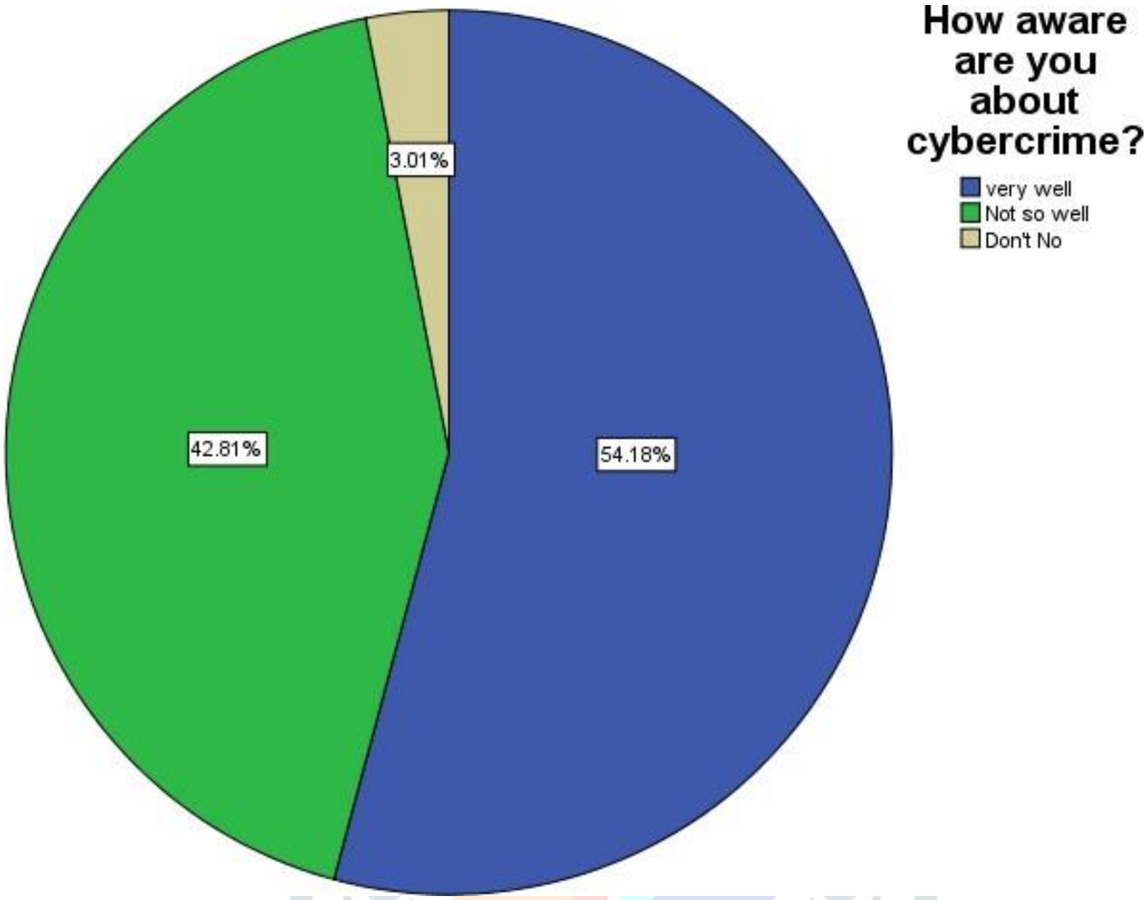

Fig No. 04

Only 54.18% people aware very well about cybercrime even 42.81% people aware not so well and 3.01% people not aware about cybercrime.

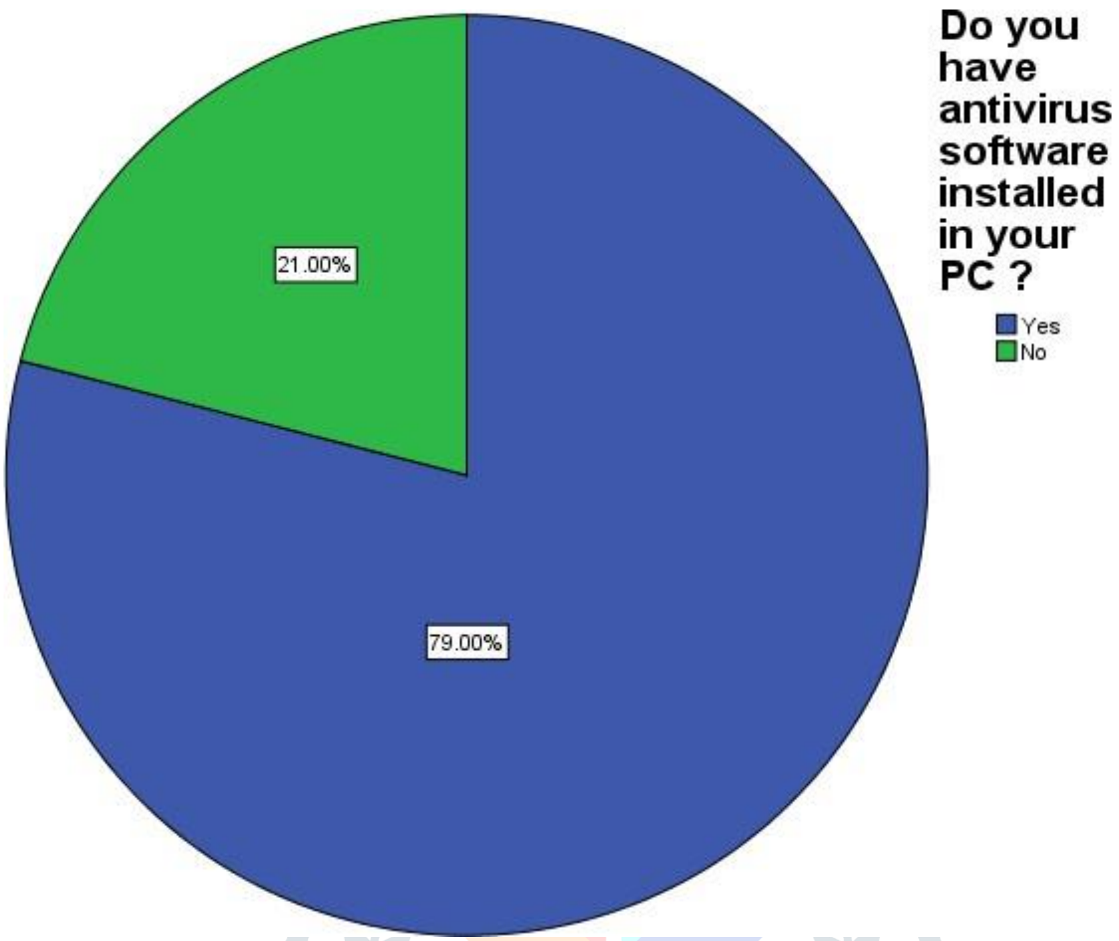

Fig. No. 05

Only 79% people have installed antivirus software in computer but 21% people have not installed.

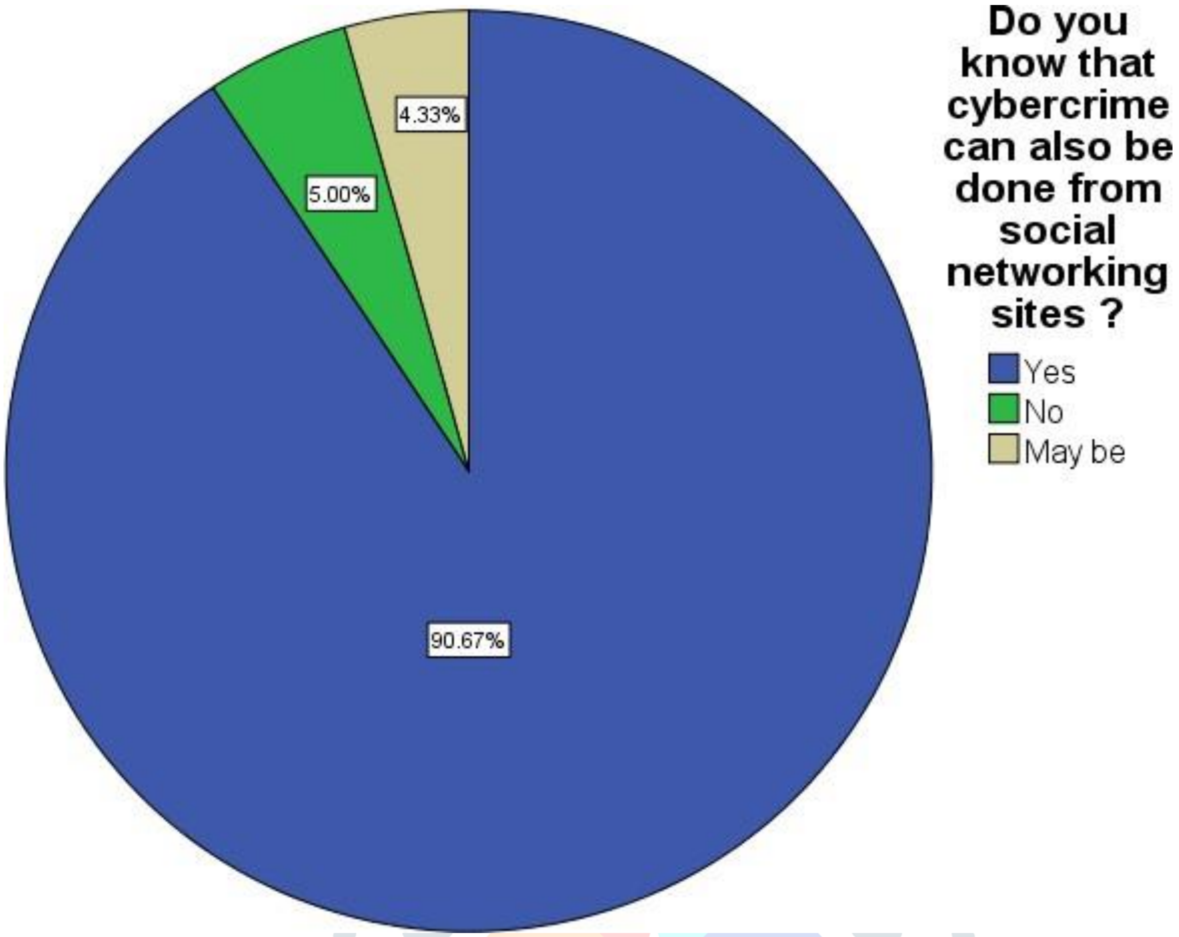

Fig. No. 06

90.67% respondents' respond that they know about cybercrime can also do from social networking sites whereas 5% people do not know and 4.33% people confused.

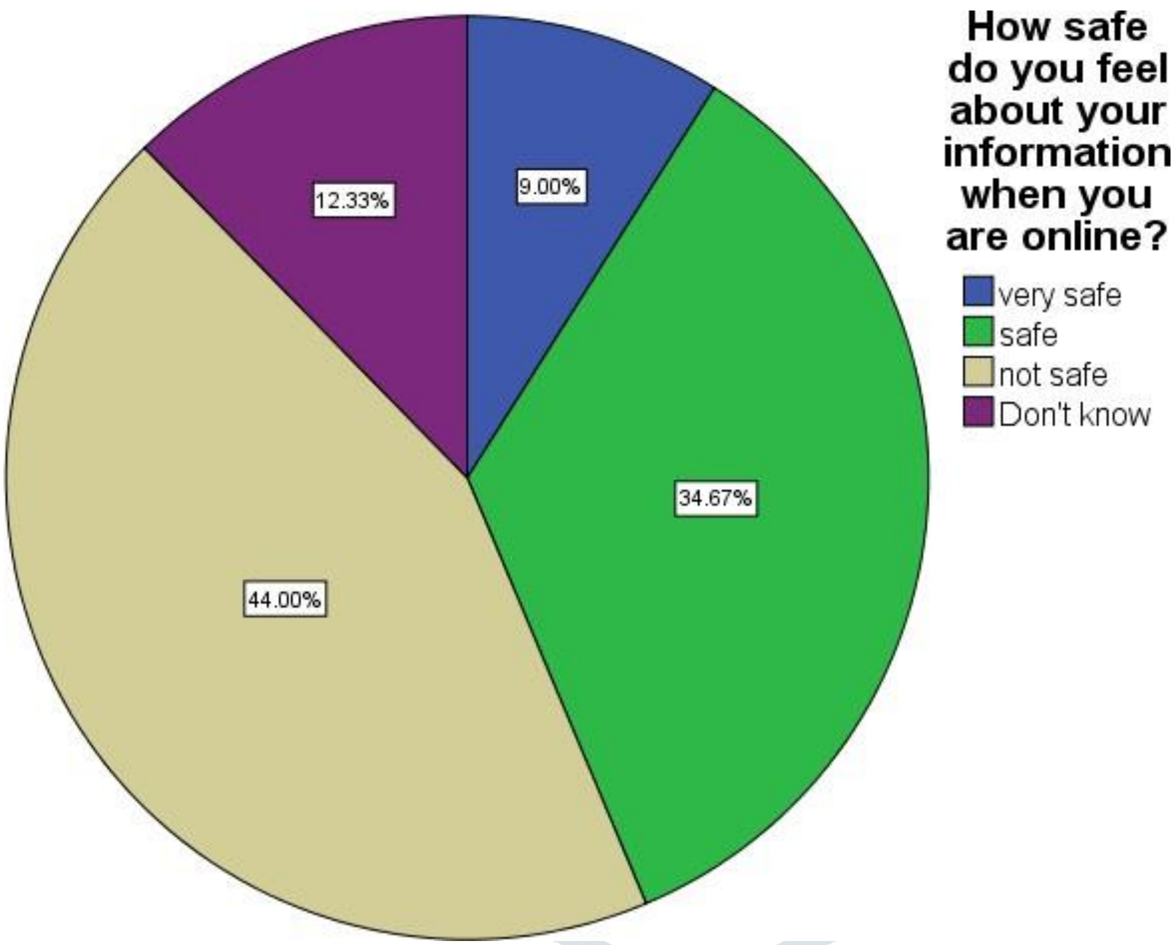

Fig. No. 07

Only 9% respondents respond that they feel very safe about the information when they are online and 44% respondents respond that they feel not safe.

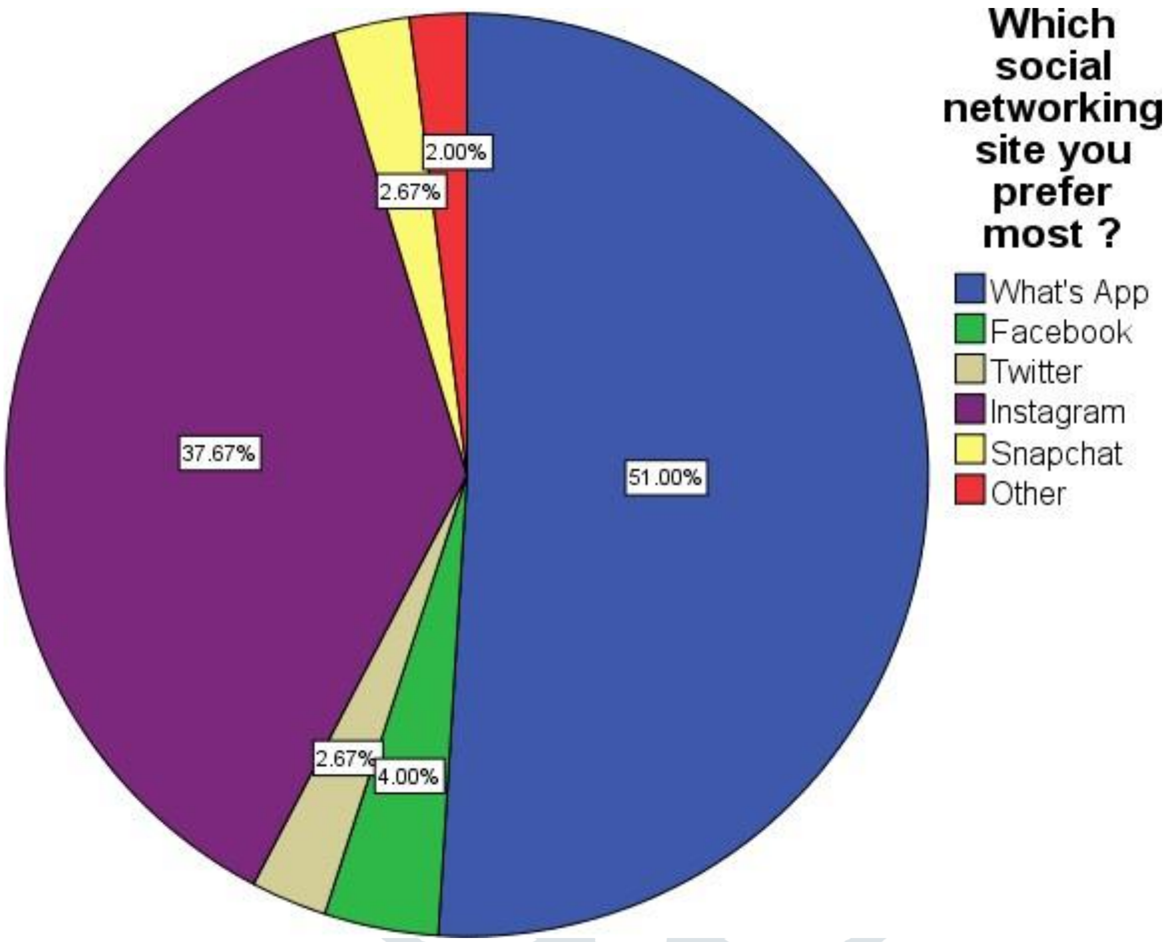

Fig. No. 08

51% people mostly prefer What's App, 37.67% people prefer Instagram mostly, 4% people prefer facebook , 2.67% people prefer twitter , again 2.67% people prefer snapchat and 2% people prefer other social networking sites.

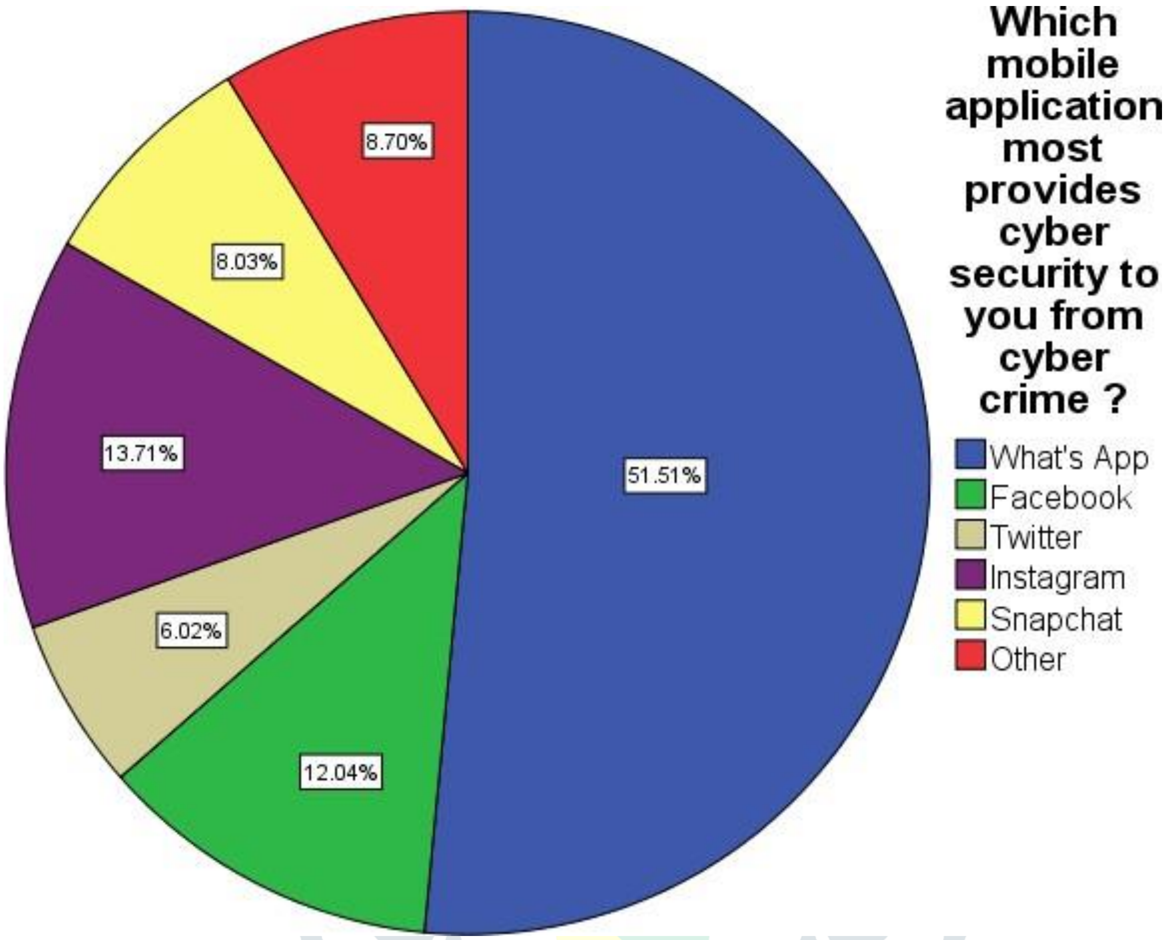

Fig. No. 09

51.51% respondents respond that What’s app provide most cyber security , 13.71 % respondents respond that Instagram provide cyber security after what’s app.

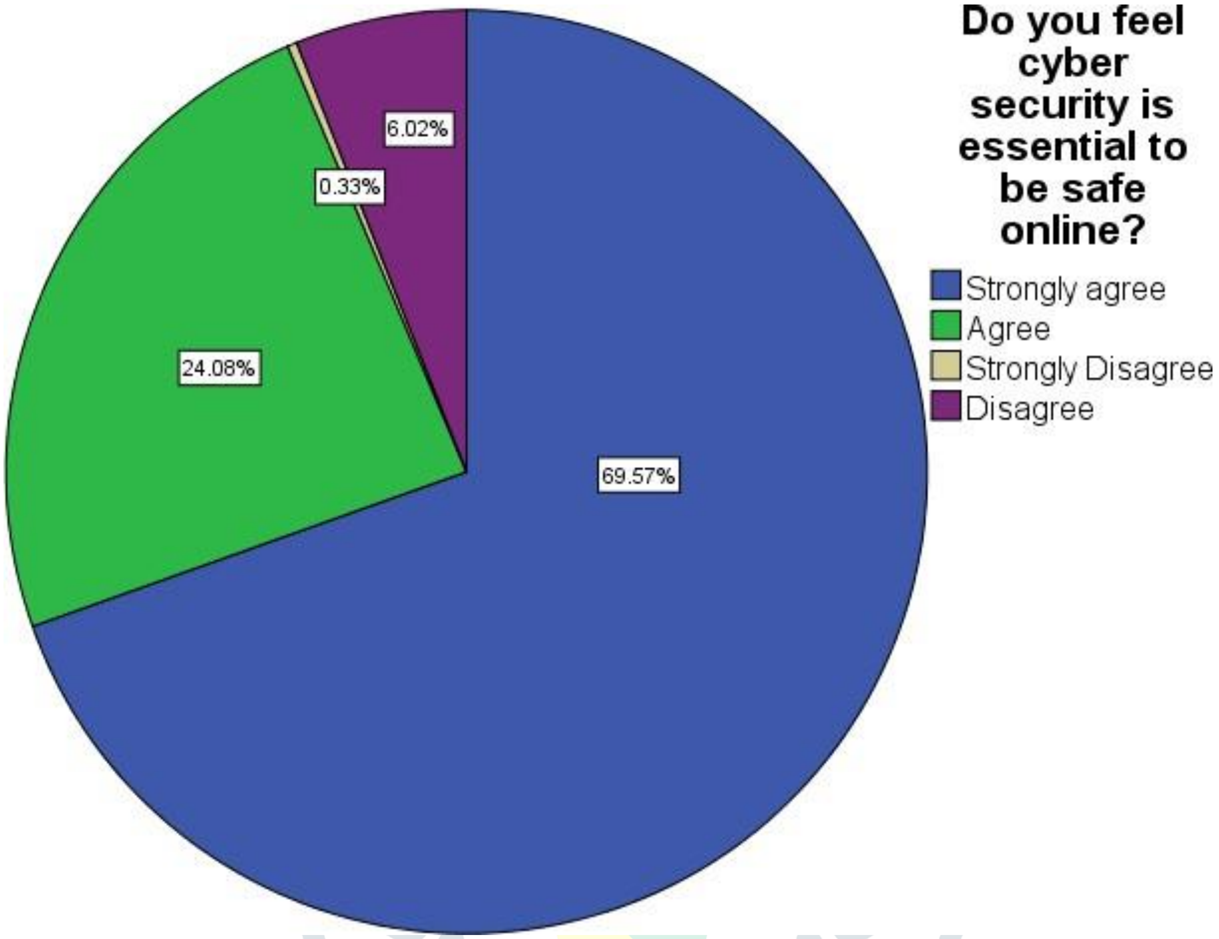

Fig. No. 10

69.57% respondents respond that cyber security is essential to be safe online.

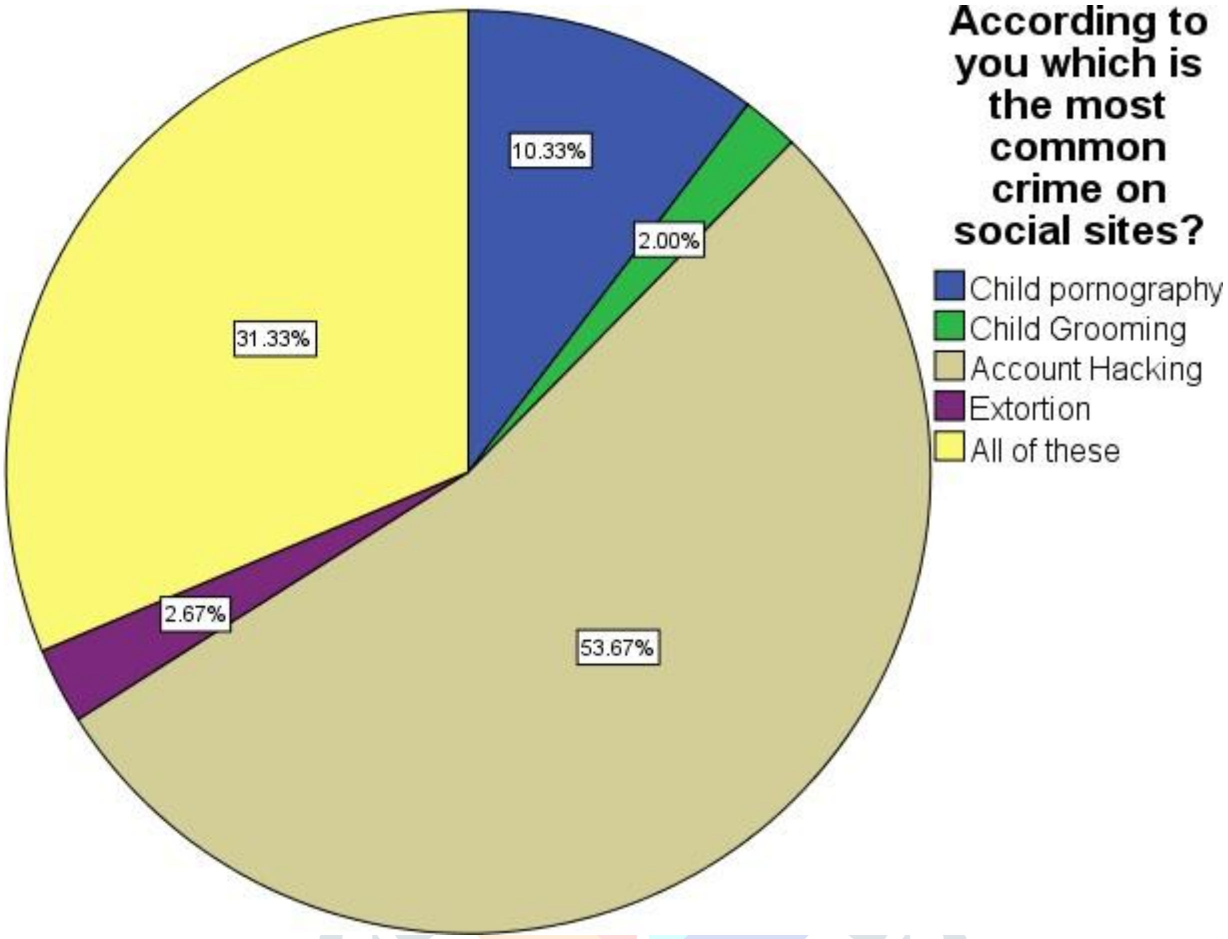

Fig. No. 11

53.67% respondents responds that Account hacking is the most common crime on social sites.

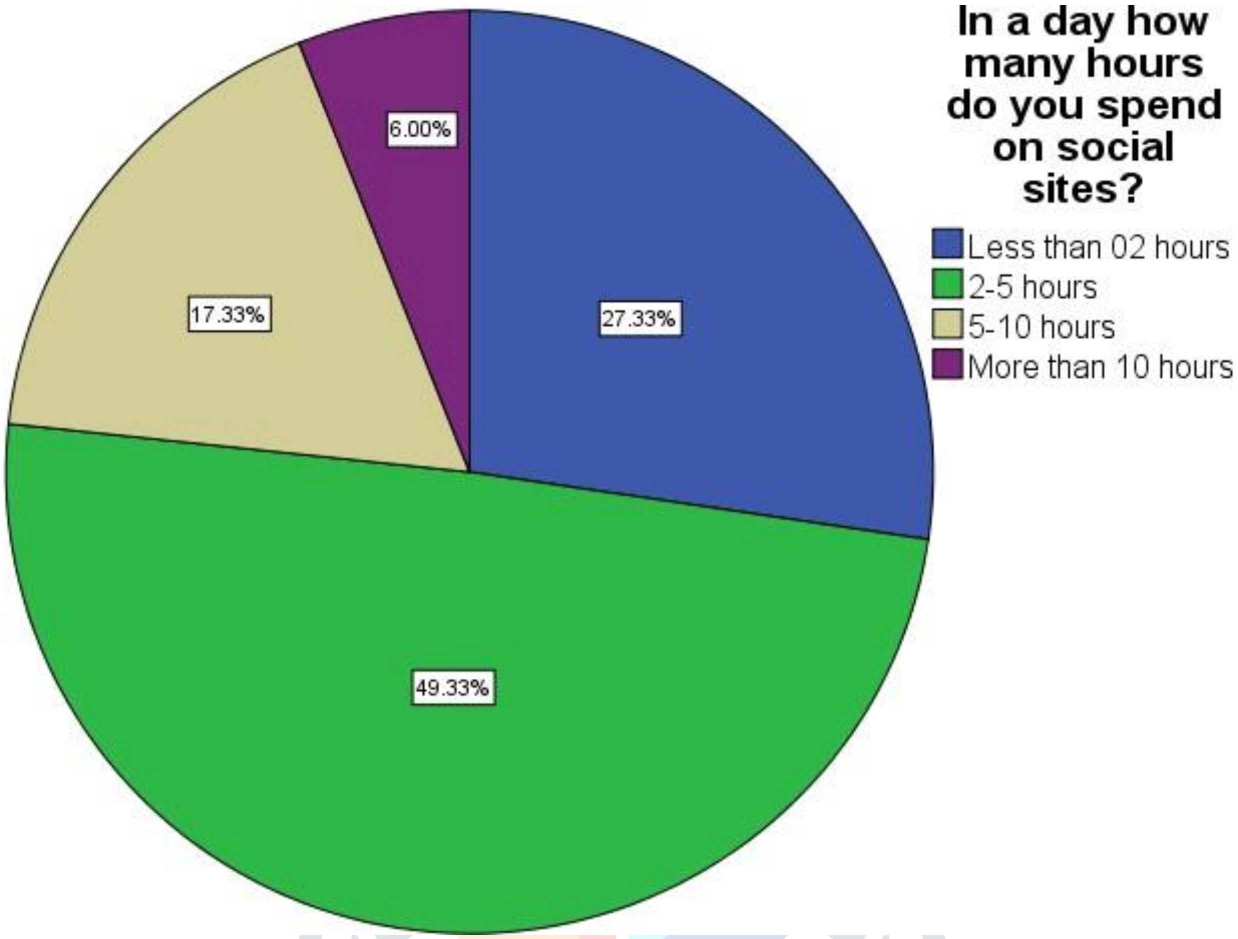

Fig. No. 12

49.33% respondents respond that they are spend 2-5 hours on social sites in a day and 27.33% respondents spend less than 2 hours on social sites.

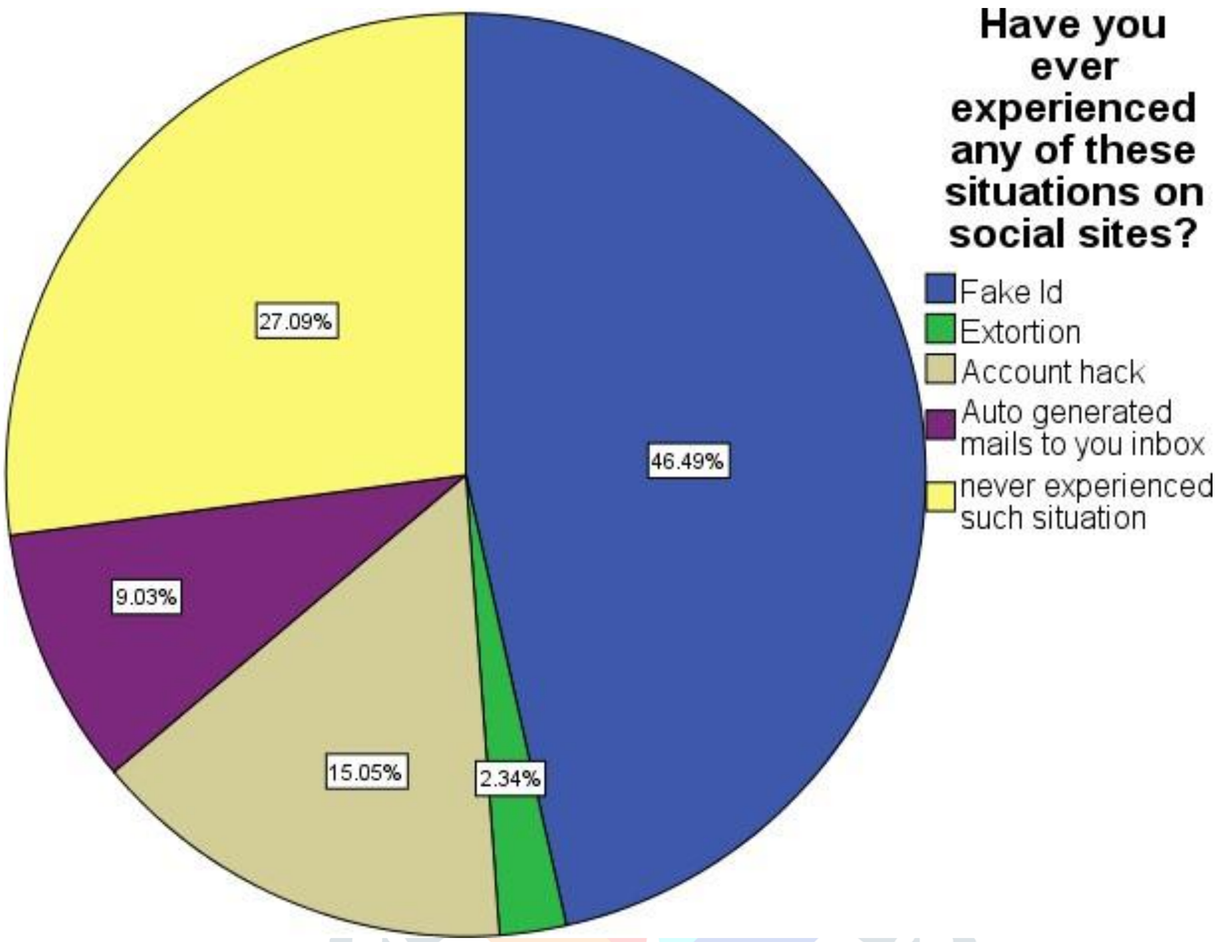

Fig. No. 13

46.49% and 27.09% respondents respond that they experienced Fake Id and account hacked situations on social sites respectively.

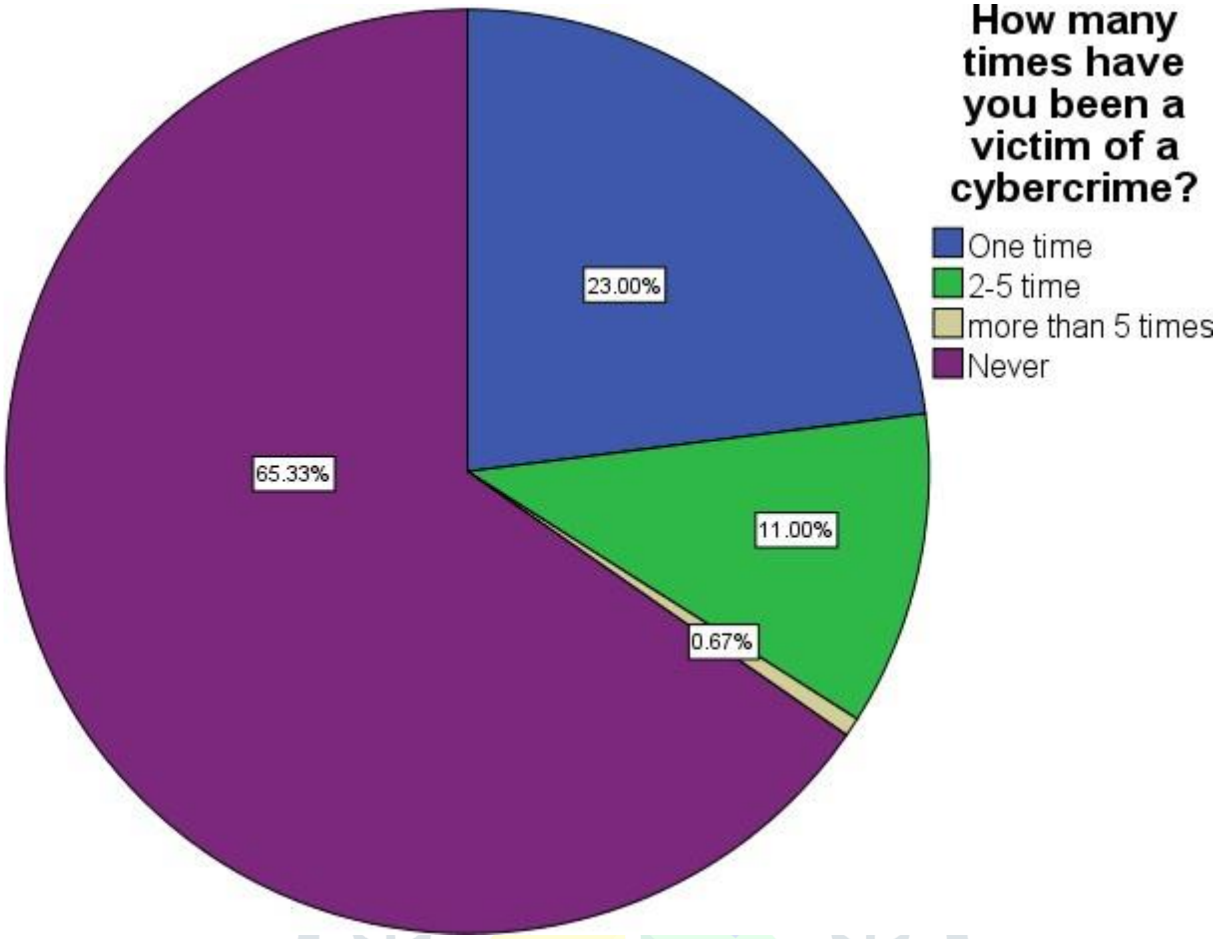

Fig. No. 14

65.33 % respondents respond that they never ever have been a victim of cybercrime but 23 % respondents respond that they have been one time victim of a cyber crime.

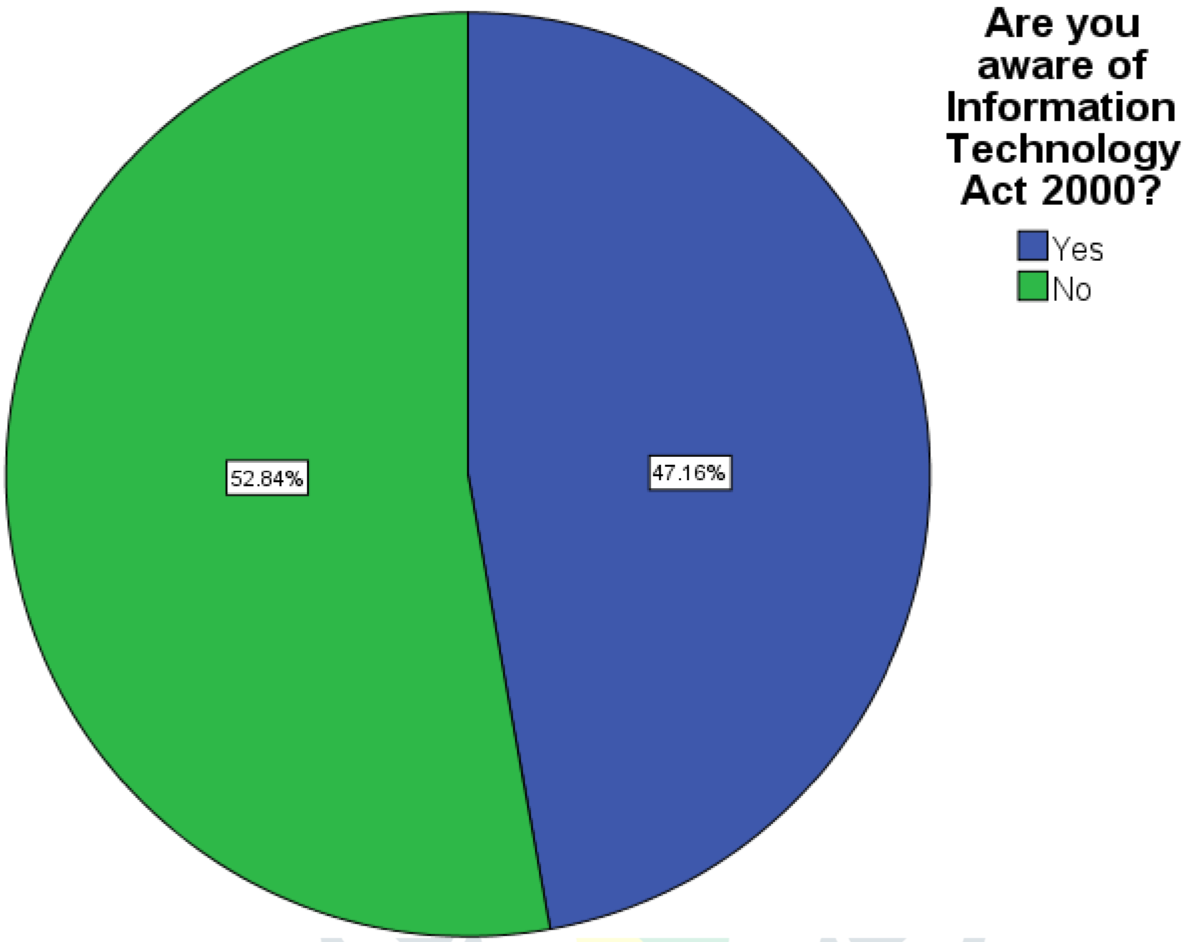

Fig. No. 15

52.84% respondents respond that they are not aware about the information technology act 2000 and only 47.16% respondents respond that they are aware about it.

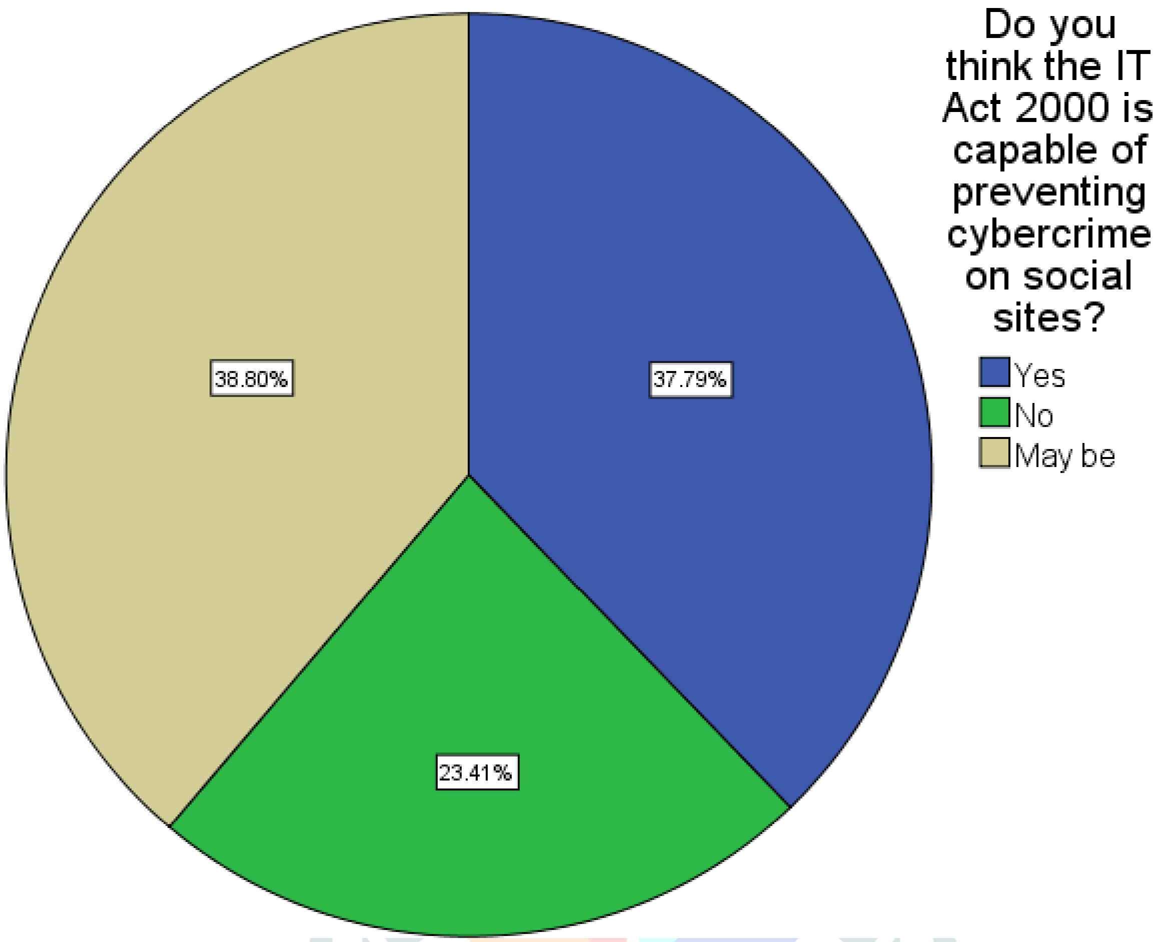

Fig. No. 16

Only 37.79 % respondents respond that the IT Act 2000 is capable of preventing cybercrime on social sites.

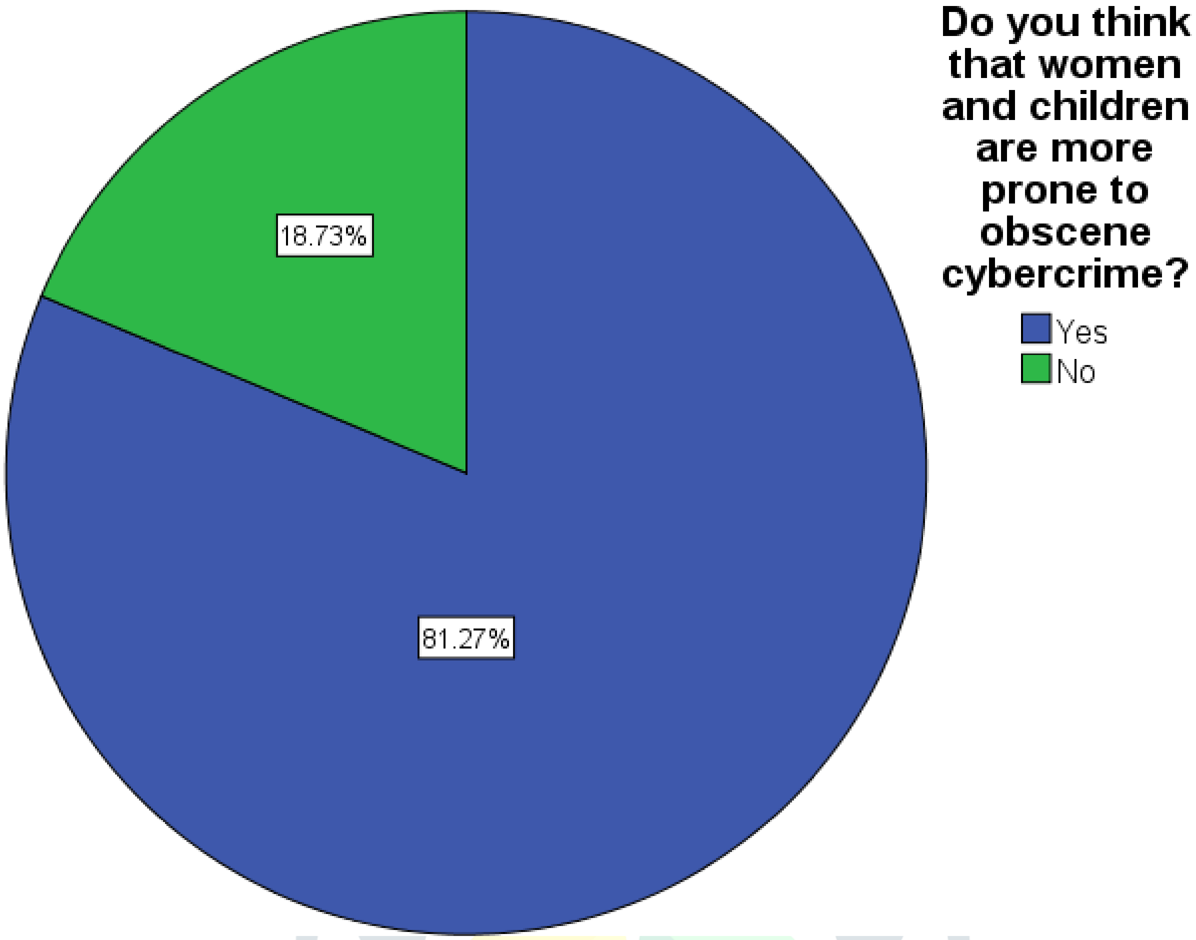

Fig. No. 17

81.27% respondents respond that women and children are more prone to obscene cybercrime.

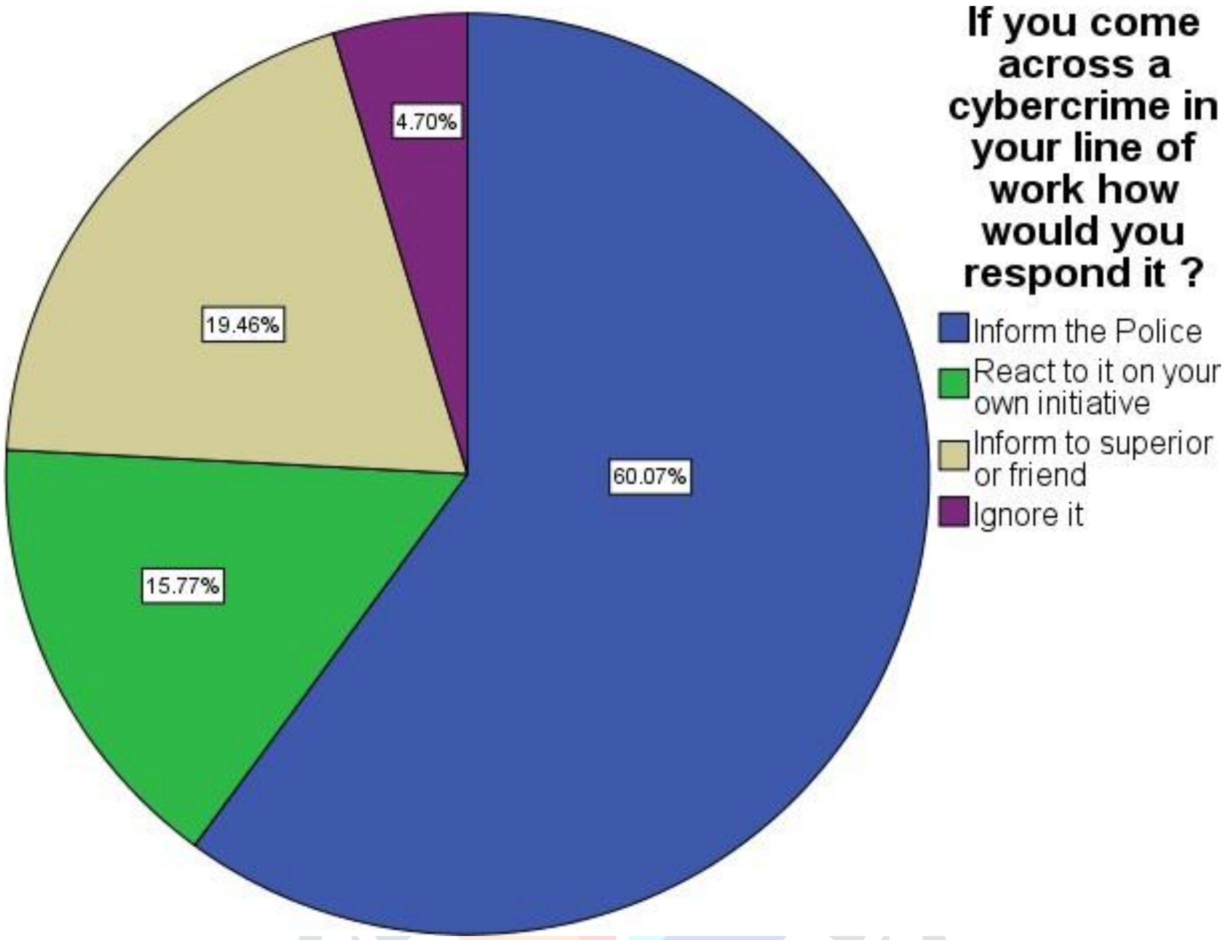

Fig. No. 18

60.07% respondents respond that they inform the police when a cybercrime in their line of work and 19.46% respondents respond that they inform to superior or friends.

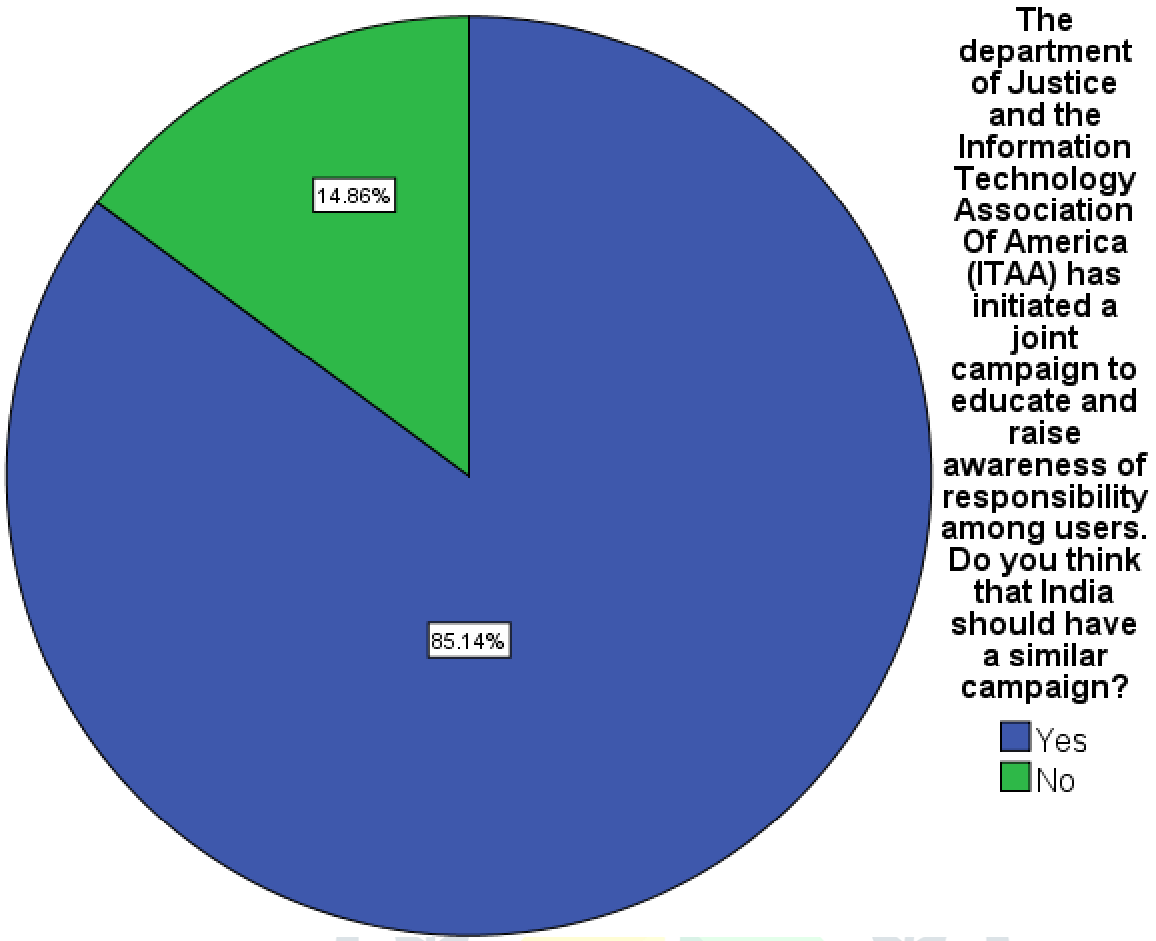

Fig. No. 19

85.14% respondents respond that government of India should have a similar campaign like an ITAA.

FINDING

In this research study the collection of the data with the help of primary as well as secondary source. Primary source (questionnaire) and secondary source (case study). Through the case study method of research found that most of the case is related to account hacking.

Through the questionnaire method of research found that only 54.18% know very well about the cyber which means there are less awareness among people about cybercrime as well as 90.67% people agree with the cybercrime can also be done from social networking sites. Besides this, study found that only 09 % people feel very safe about their information when they are online.

This Research study found that 51% people mostly using what's app to interact with each other socially. And 51.51% people agree with what's app as a mobile application that most provides cyber security from cybercrime. 69.57% strongly agree with that cyber security is essential to be safe online. And 53.67% people agree with the most common crime on social media is account hacking and 46.33% others. 49.33% people spend their time 2-5 hours in a day on social sites.

This was found out from this survey that 46.49% people have experienced related to fake Id on social sites. 65.33% people haven't a victim of a cybercrime but 23% people one times have a victim of a cybercrime. Only 37.79% people agree that IT Act 2000 is capable of preventing cybercrime on social sites means there are lack of awareness and knowledge about the IT Act 2000 and most important thing is this 81.27% people agree with that women and children are more prone to obscene cybercrime.

If a person comes across a cybercrime in the line of work so 60.07% people firstly inform the police about the issue and 19.46% people inform to superior or friends. Besides this, the data came out of this research study that 68% people agree with that India should have a similar campaign to educate and raise awareness of responsibility among user like an ITAA (Information Technology Association of America.)

CONCLUSION

All Level of cybercrime tends to overlap. Cybercrime need a computing system and hacking at same point within the process. This is often the one among the rationale that cybercrime may be a problem in today's technology based society, there's little understanding of what out there's actually a criminal offense and what's not when it involves being online. Cybercrimes goes to still grow into a bigger problem over time, if a law don't grow with the advancement of technology then issue can't be prevent associated with cybercrime. On the day to day, hackers attacked online and much of individuals are affected by cybercrime.

Be aware of any suspicious thing you see on your computing system or Mobile, never use station charger or the other public places which will cause hacking, better be using your personal power bank. Cybercrime may be a dark spot on the face of humanity. Government should start a campaign associated with educate and lift awareness among the people about the cyber crime. And even there is no any International law related to cybercrime so UN or other International Bodies should make a law or separate international organization which will work on cybercrimes. It's something which may never be totally abolished or washed faraway from social networking sites but yes if government starts listening thereto then definitely a change are often expected. Confirm you retain on removing cookies once you are online. The government should initiate campaign regarding this.

REFERENCES

1) Ahn, John (2011). The Effects of Social Network sites on Adolescents, Social and Academic Development: Current theories and Controversies. *Journal of the American Society for Information Science and Technology*, **62(8)**, 1435-1445.

2) Ahn, John (2012). Teenagers Experiences with Social Network Sites : Relationships to Bridging and Bonding Social Capital. *The Information Society* : *An International Journal*, **28(2)**, 99-109

3) Das, Biswajet and Sahoo, Jyoti (2011),Social Networking Sites. A Critical Analysis of its impact on Personal and Social life. *International Journal of Business and Social Science*, **Vol.2** (14)

4) Hetu Decary David and Morselli, Carlo (2011). Gang Presence in Social NetworkSites. *International Journal of Cyber Criminology*, July-Dec 2011, **Vol.5(2**), 876-890.

5) Mikami, Amori Yee and Szwedo, E. David and Allen, P. Joseph and Evans, M.A. and Hare L. Amanda (2010). Adolescent Peer Relationships and Behaviour Problems Predict Young Adults Communication on Social Networking Websites. *Develop. Psychology*, **46(1)**, 46-56.

6) Welsh, Jennifer (2011). Is Constant 'Facebooking' Bad for Teens? *Livescience*, 6 Aug. 2011.

7) F. Lionel (2014, June 24). IT Act 2000 – Penalties, Offences With Case Studies (Network Intelligence Global cyber security provider) https://niiconsulting.com/checkmate/2014/06/it-act-2000-penalties-offences-with-case-studies/

8) Brush Kate (2018, December). Cyber crime. https://searchsecurity.techtarget.com/definition/cybercrime

9) Types of cyber crime (2018, December) https://www.pandasecurity.com/en/mediacenter/panda-security/types-of-cybercrime/

10) Mehta Ishani J. (2014, August 23) Case study of cyber crime.
https://www.slideshare.net/ishmecse13/case-study-on-cyber-crime

11) Duggal pavan (2001, September 1). India: Cyberlaw In India: The Information Technology Act 2000 - Some Perspectives. https://www.mondaq.com/india/it-and-internet/13430/cyberlaw-in-india-the-information-technology-act-2000--some-perspectives

12) Dollarhide E.Maya (2018, March 15). Social Media. https://www.investopedia.com/terms/s/social-media.asp

13) https://www.statista.com/statistics/248074/most-popular-us-social-networking- apps-ranked-by-audience/(Accessed on June 2018)

ABOUT THE AUTHOR

Mr. MOHIT SHARMA

M.Sc. Forensic Science, CBSE NET Qualified,

Amity Institute of Forensic Science

Amity University, Sector 125 Noida Campus (Uttar Pradesh)

Mr. ROHIT SHARMA

Journalism and Mass Communication

Guru Gobind Singh Indraprastha University

New Delhi.