SOCIAL MEDIA AND CYBERCRIME AGAINST WOMEN: A STUDY OF FEMALE USERS OF SOCIAL MEDIA IN CACHAR

A THESIS

SUBMITTED TO ASSAM UNIVERSITY IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE AWARD OF DEGREE OF DOCTOR OF PHILOSOPHY IN DEPARTMENT OF MASS COMMUNICATION

Submitted By:	**Ratna Nath**
Registration No.	**10102032 of 2005 – 06**
Ph.D. Registration No.	**Ph.D./2781/15 dated 15.09.2015**

Under the Supervision of

Dr Raghavendra Mishra (Supervisor)	**Dr. Umesh Kumar (Co-Supervisor)**
Associate Professor	**Assistant Professor,**
Indira Gandhi National Tribal	**Department of Law**
University, Amarkantak	**Assam University, Silchar**

DEPARTMENT OF MASS COMMIUNICATION
ABANINDRANATH TAGORE SCHOOL OF CREATIVE ARTS AND COMMUNICATION STUDIES,
ASSAM UNIVERSITY, SILCHAR-788011

2018

Chapter-V

Summary of Findings, Conclusions and Suggestions

After the data analysis of survey research on the female users of social media in Cachar District about social media and cybercrime against women, some very important facts regarding the awareness level of female users on cybercrime issues got magnified.

This study is very useful and pertinent as well because female users of social media in Cachar District are exposed in the course of study. This helped in examining the awareness level of the female users on cybercrime issue. It is observed from the data analysis that the survey has been able to measure the awareness level of female users of social media about the various factors and threats of cybercrime.

Findings of the Study:

In the survey it is observed that 46.0% respondents from the control group and 41.0% from the experimental group are in the age group 30-35 years. Age factor is very important in the survey to observe the deviation or association among the female users of different age groups. Family association of 35.0% users from the control group consists of four members and 33.0% users of the treatment groups consists of more than four members. Survey shows that 61.0% and 67.0% users from the control and experimental groups respectively are married. Highest level of education as noted are 62.0% and 68.0% users from the control and experimental groups respectively are Post Graduate.

Survey shows that 41.0% and 36.0% users from the control and experimental groups respectively are private employed. 38.0% and 33.0% of the respondents from both the groups fall in the income limit above Rs. 60,000. 39.8% and 33.0% of the users from both the groups are using smart phone for 3-4 years. But in the post-test survey it is observed that the usage time of 3-4 years is reduced to 38.5% in the control group and 32.7% in the experimental group. As observed in the pre-test survey, 45.2% of the users in the control group spend time on their smart phone for 3-4 hours in a day while 42.3% of the users in the experimental group spend time for 1-2 hours in a day. But in the post-test survey the usage time of 3-4 hours is reduced to 43.8% in the control group and 41.8% in the experimental group for 1-2 hours.

Female social media users are one of the group of end users of social media. They need to have the knowledge about social media and its associated risk. Various types of cybercrimes are being performed in the social media platform. Devices connecting to the internet and the mode of internet connection are the most common tools to commit cybercrimes. The survey shows that personal computer, laptop, smart phone and tablet are the devices connecting to the internet. Among these devices smart phone is rated high with 93.0% and 87.0% in the control and experimental groups respectively in the pre-test survey and 96.0% and 88.0% in the post-test survey. It refers to the portability factor of the devices that is being used by its users to use it in their convenient way.

The survey shows that broadband connection, data card, wi-fi connection and mobile data are the available internet connections to connect data to their devices. Among these connections mobile data is used by 91.0% and 57.0% of the users in the control and experimental groups respectively in the pre-test survey and 94.0% and 58.0% in the post-test survey. It symbolizes the portability factor of the mode of internet connection to connect data to the devices.

The survey shows that video chatting is not very popular among the respondents. It is observed that not every respondent does video chat. In the pre-test survey it is found that 98.9% of the users in the control group and 88.2% of the users in the experimental group does video chat with their family. After the exposure to treatments in the experimental group the response to video chat circle remains the same with 97.8% of the users in the control group and 90.6% of the users in the experimental group.

The survey shows that chatting is very popular among the respondents. It is observed that not every respondent does chat. It is observed that 98.9% of the users from the control group and 100% of the users from experimental group does chat with their friends. After the exposure to treatments in the experimental group the chat circle remains the same with 100% response rate in both the groups.

The survey shows that every respondent is associated with social media sites. In social media sites there are some options provided in accordance to the response to friend request. It is observed in the pre-test survey that 59.8% of the users from the control group and 44.4% of

the users from the experimental group use to ignore the friend request which seems to be fake or unknown. But after the exposure to treatments in the experimental group the responses to accepting fake friend request remains the same but the rate decreases to 52.3% in the control group and 43.1% in the experimental group.

Social media sites have privacy setting option that can be synchronized according to the users' choice. The pre-test survey shows that 46.0% of the users from the control group and 61.0% of the users from the experimental group have synchronized their privacy setting to public. After the exposure to treatments in the experimental group the response to privacy option remains the same but the response rate decreases to 48.0% in the control group and 47.0% in the experimental group.

Threat is a type of cybercrime. Those who have online account or smart phone may receive threat through e-mail or message or by some other means of communication. From the pre-test survey it is observed that not every user have received threat. In response to threat, 60.6% of the users from the control group and 55.0% of the users from the experimental group used to ignore. But after the exposure to treatments in the experimental group the response to threat remains the same with the decrease in the response rate to 61.1% and 61.4% in the control and experimental group respectively.

Cyber criminals often post sexually explicit materials to any public profile through social networking sites. The pre-test survey shows that very few of the users have received such content till the survey is done. 93.8% of the users from the control group and 67.9% of the users in the experimental group used to report spam on receiving such content. After the exposure to treatments in the experimental group the response to sexually explicit materials remains the same but the rate changes to 100.0% in the control group and 78.6% in the experimental group.

In social networking sites there is a provision of posting pictures in the display of their profile as their identity. Multiple users can be of the same name but the display picture will help to identify the exact person in the social media. From the pre-test survey it is found that the rate for posting their own picture as display picture decreases from 97.0% to 95.0% in the control group and in the experimental group after the exposure to treatment it decreases from 90.0% to 84.0%.

But few of the respondents do not post their own picture in the display of their social media profile. The reason found in the survey is hesitation for both the groups. In the pre-test survey the response rate was 100% in the control group and 40.0% in the experimental group. But after the exposure to treatments in the experimental group the response rate is found as 80.0% in the control group and 87.5% in the experimental group.

Social media sites have privacy setting option for every social media activities and that can be synchronized according to the users' choice. From the survey it is observed that not all the users share their pictures with others. The pre-test survey shows that 80.6% of the users in the control group and 76.5% of the users in the experimental group keep their privacy setting to friends only. But in the post-test survey the rate reduces to of 79.7% in the control group and 73.1% in the experimental group.

In the social media any users can comment on the picture shared by any other social media user. It is possible for any user to post vulgar comment on the shared picture. In the survey it is found from both the groups that only a small portion of the respondents have received vulgar comment till the survey is done. In response to the comment majority from both the groups have chosen the option block the user. In the pre-test survey the rate is found to be 80.0% in the control group and 77.8% in the experimental group. But in the post-treatment survey it is found to be as 83.3% in the control group and 77.8% in the experimental group and the response to vulgar comment remains the same.

It is important to have antivirus installed in the devices connecting to the internet to stay safe and have secure surfing. It is equally important to update antivirus for better protection from the unwanted problems that incurred while using internet. The pre-test survey shows that 45.0% of the users in the control group update their antivirus yearly and 36.0% of the users in the experimental group update monthly. In the post-test survey the response to frequency of updating anti-virus is found to be the same as of pre-test in both groups and the response rate is 45.0% in both the groups.

Almost every place is under the surveillance of wi-fi now a day. Some of them are not restricted by password for public usage. People access it whether they are aware or not of the negative sides of the public wi-fi usage. From pre-test to post-test survey it is found that users

access to public wi-fi and the response rate is increased from 16.0% to 18.0% in the control group while in the experimental group the rate is decreased from 26.0% to 22.0%.

From both the surveys it is found that majority of the respondents in both the groups do not sure about the risk of accessing public wi-fi. From pre-test to post-test survey it is evident that the response rate is decreased from 64.0% to 62.0% in the control group and 59.0% to 56.0% in the experimental group.

In social media cybercrime is mostly deviated towards women. Various reasons are there to justify the plot. In the pre-test survey the reason is found to be women are easier to convince in both the groups. In the control group the response rate is 55.0% and in the experimental group the rate is 43.0%. In the post-test survey the reason is same as that of earlier survey and the rate is 57.0% in the control group and in the experimental group the rate is 52.0%.

Downloading software or movies from an unauthorized source is considered piracy. Piracy is another type of cybercrime. From both the surveys it is observed that the response rate increases from 68.0% to72.0% in the control group and 59.0% to 75.0% in the experimental group. They gave their preference to buy from authenticated sites for downloading software and movies.

Cyber law has been introduced as Information Technology Act-2000 to prosecute the cyber criminals. From both surveys it is observed that users have knowledge about the existence of cyber laws and the response rate increases from 70.0% to 72.0% in the control group and in the experimental group the rate increases from 78.0% to 95.0%.

Social networking site is a platform that provides public exposure of personal information. These sites are interactive in nature. Such features attract different illegal activities to perform. The pre-test survey shows that 45.0% of the users from the control group and 57.0% of the users from the experimental group have disagreed with the statement. In the post-test survey 38.0% and 61.0% of the users from the control and experimental group respectively have disagreed with the statement.

Social networking sites provide a platform for sharing every details about a user. Such features attract different illegal activities like cyber stalking. The pre-test survey shows that

57.0% and 68.0% of the users from the control and experimental group have agreed with the statement. In the post-test survey 59.0% and 58.0% of the users from the control and experimental group have agreed with the statement.

Chat with online friends revealing personal details of the users can make them a target or even they may become a victim of many types of crimes. Online friends may use the personal information for committing crimes or may harass them leading to psychological or physical harm. From the pre-test survey it is observed that 51.0% and 39.0% of the users from the control and experimental group respectively have agreed with the statement. In the post-test survey 47.0% of the users from the control group have agreed and 46% of the users from the experimental group have strongly agreed with the statement.

Social networking sites are online platform for interaction and communication with the world. Users can interact with anyone from anywhere without appearing physically to make interaction with them. It is a cyber space where everything is real in a virtual way. From the pre-test survey it is observed that 76.0% of the users from the control group and 82.0% of the users from the experimental group have agreed with the statement. In the post-test survey 63.0% and 72.0% of the users from the control and experimental group respectively have agreed with the statement.

In social networking sites anyone can make social media profile. Therefore there is every chance of making fake profile and send friend request with an evil intension. Accepting unknown friend request without proper knowledge lead to a very dangerous situation. From the pre-test survey it is observed that 50.0% of the users from the control group have strongly agreed and 59.0% of the users from the experimental group have agreed with the statement. In the post-test survey 49.0% of the users from the control group have agreed and 53.0% of the users from the experimental group have strongly agreed with the statement.

In social networking sites users post their details and pictures. These pictures can be downloaded and used in illegal and anti-social activities. Morphing is a cybercrime where pictures are cropped and uploaded in the adult sites. From the pre-test survey it is observed that 57.0% of the users from the control group and 64.0% of the users from the experimental group have agreed with the statement. In the post-test survey 60.0% and 50.0% of the users from the control and experimental group respectively have agreed with the statement.

Teenagers are techno savvy group of people. They enter into the virtual world of communication through social networking sites. They frequently use the computer and internet without having proper knowledge about the safety and security of the using pattern. Security issues while accessing internet or using computer have to be increased among them to combat cybercrimes. From the pre-test survey it is observed that 62.0% of the users from the control group and 53.0% of the users from the experimental group have agreed with the statement. In the post-test survey 58.0% of the users have agreed while 52.0% of the users from the experimental group have strongly agreed with the statement.

Emergence of social networking sites has initiated many types of online crimes. In the sites anyone can be traced and can become the easy target by being friendly with them. Online predator offer attractive job opportunities and suitable career opportunities to the online users making them trapped and victims of trafficking. From the pre-test survey it is observed that 72.0% of the users from the control group and 62.0% of the users from the experimental group have agreed with the statement. In the post-test survey 75.0% and 66.0% of the users from both the group respectively have agreed with the statement.

In the social networking sites information and pictures are exposed publicly. Using such information evil minded people can create fake accounts to perform various illegal tasks. From the pre-test survey it is observed that 58.0% of the users from the control group and 66.0% of the users from the experimental group have agreed with the statement. In the post-test survey 56.0% and 61.0% of the users from both the group respectively have agreed with the statement.

Social networking sites are interactive in nature. Anonymity factor of the sites makes it very convenient for the users to perform their task without any intervention. From the pre-test survey it is observed that 59.0% of the users from the control group and 60.0% of the users from the experimental group have agreed with the statement. In the post-test survey 57.0% of the users from the control group have agreed and 52.0% of the users from the experimental group have strongly agreed with the statement.

Bullying is same as harassment but with minor difference. Traditional bullying is the cybercrime when incorporated with the new media technology it turns out to be cyber bullying. It generally targets teenage people also committed by the teenage people. From the pre-test

survey it is observed that 55.0% of the users from the control group and 60.0% of the users from the experimental group have agreed with the statement. In the post-test survey 57.0% and 60.0% of the users from both the group respectively have agreed with the statement.

Computer virus is a computer generated program designed with the intension to destroy any system or to steal data from the system. The program is generated in a way that once a system gets affected with virus anything connected to it gets automatically damaged. From the pre-test survey it is observed that 62.0% of the users from the control group and 55.0% of the users from the experimental group have agreed with the statement. In the post-test survey 65.0% of the users from the control group and 63.0% of the users from the experimental group have agreed with the statement.

In social networking sites there is a feature to display present location of the user. Anyone can be stalked easily by tracing the location displayed in the social media profile. Cyber stalking is a possible risk associated with that feature. From the pre-test survey it is observed that 76.0% of the users from the control group and 72.0% of the users from the experimental group have agreed with the statement. In the post-test survey 77.0% of the users from the control group and 73.0% of the users from the experimental group have agreed with the statement.

With the advent of digital technology anyone can access illegally to any system may it be personal information or webcam of personal computer. In every technological device there are some loop holes which is impossible to traceable. Hackers take this to their advantage to access into any device or any system. When they hack a system it is possible to gain access anything attached to it. From the pre-test survey it is observed that 47.0% of the users from the control group and 48.0% of the users from the experimental group have agreed with the statement. In the post-test survey 48.0% of the users from the control group and 57.0% of the users from the experimental group have agreed with the statement.

Technology makes everything secure and equally vulnerable. Therefore it is very essential to keep them secure by password protection. Easy password can be traced very easily so it should be very complex and long with the combination of numbers, letters and alpha numeric symbols to make it untraceable. From the pre-test survey it is observed that 56.0% of the users from the control group and 53.0% of the users from the experimental group have

agreed with the statement. In the post-test survey 56.0% of the users from the control group and 51.0% of the users from the experimental group have agreed with the statement.

Computer and internet are the new media technologies used in every sections of life. These two are inevitable for performing any day to day task. But operating any device or using any technology without proper knowledge is dangerous. Awareness can help from becoming a victim of cybercrime. From the pre-test survey it is observed that 55.0% of the users from the control group and 70.0% of the users from the experimental group have agreed with the statement. In the post-test survey 55.0% of the users from the control group and 65.0% of the users from the experimental group have agreed with the statement.

Emergence of new media has created many crimes known as cybercrimes. It is a crime committed with technology like computer. Again the crime targets computer for their illegal purpose. From the pre-test survey it is observed that 54.0% of the users from the control group and 70.0% of the users from the experimental group have agreed with the statement. In the post-test survey 55.0% of the users from the control group and 68.0% of the users from the experimental group have agreed with the statement.

Online predators programmed software to hack into system or spreading virus or malware. They send it by various means to attract people to fall into their prey. In one way they send it like pop up messages or embedded link in different website pages. Clicking on the suspicious link may be dangerous. From the pre-test survey it is observed that 60.0% of the users from the control group and 73.0% of the users from the experimental group have agreed with the statement. In the post-test survey 62.0% of the users from the control group and 66.0% of the users from the experimental group have agreed with the statement.

Using internet without security may be lead to a dangerous situation. Many online crimes are done by using internet. Malicious programs are send by different links appeared while opening a website. Internet security scans all the links on clicking on it. From the pre-test survey it is observed that 56.0% of the users from the control group and 64.0% of the users from the experimental group have agreed with the statement. In the post-test survey 61.0% of the users from the control group and 63.0% of the users from the experimental group have agreed with the statement.

Crimes that are performed by using new media technologies like computer and the internet are cybercrimes. It is similar to traditional crimes but with a little difference of the involvement of new media. From the pre-test survey it is observed that 47.0% of the users from the control group and 42.0% of the users from the experimental group have agreed with the statement. In the post-test survey 50.0% of the users from the control group and 58.0% of the users from the experimental group have agreed with the statement.

In social media photo tag is a feature for spreading photos with many profile users. Tagged photo can be seen by all the listed friends of those tagged friends. It is possible to download photo by those users and use it as a fake identity. From the pre-test survey it is observed that 41.0% of the users from the control group and 46.0% of the users from the experimental group have agreed with the statement. In the post-test survey 43.0% of the users from the control group and 50.0% of the users from the experimental group have agreed with the statement.

Profile and wall pictures of social media can be downloaded and used for various crimes like morphing, identity theft or harassment. More and more cybercrimes are deviated towards female users and so the pictures can play a vital role for committing such crimes. From the pre-test survey it is observed that 40.0% of the users from the control group and 48.0% of the users from the experimental group have agreed with the statement. In the post-test survey 45.0% of the users from the control group and 59.0% of the users from the experimental group have agreed with the statement.

Shared photo on social media can be downloaded and used for various crimes like morphing, extortion and identity theft. More and more cybercrimes are deviated towards female users and so the pictures can play a vital role for committing such crimes. From the pre-test survey it is observed that 48.0% of the users from the control group and 65.0% of the users from the experimental group have agreed with the statement. In the post-test survey 52.0% of the users from the control group and 66.0% of the users from the experimental group have agreed with the statement.

Map application on the social networking sites indicates the present location of the user. Anyone can stalk the user with the help of geo location shared by the users. Map application is a geo social location tracing application that helps a user sharing their present

location. From the pre-test survey it is observed that 75.0% of the users from the control group and 67.0% of the users from the experimental group have agreed with the statement. In the post-test survey 76.0% of the users from the control group and 73.0% of the users from the experimental group have agreed with the statement.

In social networking sites many fake profiles are created to cheat people. Anything posted in their profile without having much knowledge about the user may be dangerous as being a victim of cybercrime. From the pre-test survey it is observed that 58.0% of the users from the control group and 59.0% of the users from the experimental group have agreed with the statement. In the post-test survey 60.0% of the users from the control group and 61.0% of the users from the experimental group have agreed with the statement.

In social media users can post their personal information like the events and happenings of their personal life. This information can be misused for committing several crimes. Mixed reactions are found in the survey. From the pre-test survey it is observed that 48.0% of the users from the control group and 59.0% of the users from the experimental group have agreed with the statement. In the post-test survey 58.0% of the users from the control group and 67.0% of the users from the experimental group have agreed with the statement.

In video chat the video can be recorded and the photo can be taken with the advent of technology. These video and photos can be stored for performing various online crimes. From the pre-test survey it is observed that 68.0% of the users from the control group and 60.0% of the users from the experimental group have agreed with the statement. In the post-test survey 70.0% of the users from the control group and 67.0% of the users from the experimental group have agreed with the statement.

Statistical tests were performed to check if there is any discrepancy between the data gathered from the two groups. Paired t-test was performed to compare the average score of the pre-test and post-test of the control group. The value of the test statistics was 1.236 (p-value 0.219) indicating that the difference in the average for the Pre-test and post-test of the control group do not differ significantly. Hence we accept our null hypothesis.

Paired t-test was performed to compare the average score of the survey done before and after providing treatments to the experimental group. The value of the test statistics was 13.809

(p-value 0.000) indicating that the difference in the average for the survey done before and after providing treatments differ significantly. Hence we reject our null hypothesis.

Two independent sample t-test was performed to compare the average score for both the pre-test of control and experimental group. The value of the test statistics was 1.531 (p-value 0.129) indicating that the difference in the average for both the pre-test of two groups do not differ significantly. Hence we accept our null hypothesis.

Two independent sample t-test was performed to compare the average score for the post-test of control group and post-test done after providing treatments to the experimental group. The value of the test statistics was 12.969 (p-value 0.000) indicating that the difference in the average for the post-test of control group and post-test done after providing treatments to the experimental group differ significantly. Hence we reject our null hypothesis.

Conclusions:

After the data analysis of survey research about social media and cybercrime issues with the exposure to female users of social media in Cachar District, it can be ascertained that the survey has been able to measure the awareness level of the users on cybercrime.

In reference to the **first objective,** from the study it is observed that the nature of cybercrime is technologically advanced. Many crimes are committed daily all over the world through digital technology and people who are not aware of the risk of cybercrime are often getting victimized. Even if they are aware of such crimes, the chances of being victimized would not be less because the technology associated with it is very advance and fast changing. The Information Technology has succeeded to maintain the speedy growth of cybercrime. Criminals have managed to use computer, internet and mobile phones in the commission of traditional crimes in a new dimension.

The nature of cybercrime is highly intricate, self-strengthening, technically advanced, speedy, geographically widespread and haphazard. Earlier cybercrime was committed by any individual or a small group of people. But now technically advanced cybercrime are supervised and operated with specially trained professional. The network of cyber-criminal are very complex and they come up together to commit crimes on an unprecedented scale.

Intensity of cybercrime is strong on Social media. Internet and social media are growing parallel to each other as large number of technologies; social networking sites and interactivity tools have turned out to be more prominent. In most of the cases it has been observed that ignorance of the people towards the technology causes risk in their life. Internet is playing a vital role in sharing information as well as spreading virus. Therefore social media as a part of online media is not a risk free zone.

Computer based crime has become very prevailing as the crime moves away from the traditional method of committing crimes. Social media and other internet based technology has very attractive feature that can attract anyone irrespective of their age, education, income, employment status of them. New media technologies are becoming very advanced in modifying their technologies as it has miniaturized each and every devices. Miniaturization of

technologies have made the utility factor very convenient and portable to use. Smart phone is social media friendly and very pertinent for the users to use it from anywhere. Portable Internet connection is easy to carry and hence the users are free to move in any place being online.

Due to the negative impact of cybercrime many activities on social media are not considered safe for female users. Female social media users draws a restriction line for doing online chat and video chat. Female users become pessimistic while accepting an unknown friend request. They keep their social media profile restricted to the known region only. The worst frightening aspect of cybercrime falls on the female users of social media. Threat, posting sexually explicit material or content into their profile, posting vulgar comment are the main negative impacts of cybercrime on the female users. Due to such adverse effect of cybercrime, female users hesitate to post their own picture in their social media account. If they do so, they restrict the profile and do not accept any unknown friend request. They even have a constant fear of sharing their personal pictures and videos with others. Such frightening aspect may lead a woman to the extreme depression up to the level of harming them psychologically or physically.

In reference to the **second objective,** social networking sites are the most vulnerable areas to the cybercrime related issues amongst all social media. Cybercrime has the potential to crack into the general system but also into the life risk. Online communication portals is in the danger zone of cybercrime. Social media is no more a safe platform for women to connect, communicate or share anything like personal opinions, pictures, videos, displaying present location, occupation or any social media activities. Female users of social media suffers mostly by the various types of cybercrimes designed specially to target women. Social media users may fall into the trap of cybercriminal at any step

However, it has been anticipated that advanced level of cyber-attacks in social media against women will be able to pull out a user's information such as contacts, present location and current activities. This information can further be used in various illegal and anti-social activities. Many alluring offers comes as spam messages, pop-ups and social media advertisements are another cyber-attacks that tricks the user into revealing authentication credential in the pretext of some identified websites. Phishing is a technique that is used as

social engineering attack to steal personal information. Users should stay alert to any request appears as "urgent" from the site to reset any password. Phishing attacks is a vector for numerous attack that are to a user's detriment such as: identity theft, data theft, spreading virus, disruption of a system and reputation damage.

Surfing social media sites using public wi-fi increases the vulnerabilities of social media in cybercrime. In many cases the hacker send a spoofed website much similar to an original website. Clicking on the site may direct to a hoax site leading to breaking down to the users' key information. Female users of social media are well educated techno savvy people. But the users mostly keep their privacy setting as public. Some users never mind to use public Wi-Fi and they do not aware of the risk involved with it. Some even are skeptical about the risk associated with using public Wi-Fi. Some users never update their anti-virus at all. In video chat identity cannot be hidden to the users and screen shot of the users can be taken. It can further be used for harassment. Sharing location on social media profile can cause stalking. Photo tagging is a major threat to cyber-attack. With the tagging of a photo a user of a user can follow a chain of tagged photos referred as cluster to reach all the users related to that user and free to use all such information at its end.

In reference to the **third objective,** it is evident from the study that most of the female users are aware about the consequences of cybercrime. The study shows the awareness level of female users of social media and how they incorporate social media in their day to day life. In the outset both the groups do not have in depth knowledge about the consequences of cybercrime in social media and how it is operated through social media. They do not consider cybercrime as a serious issue unless the problem arises to them. Performing various social media activities without knowing the negative impact of cybercrime which is operated through social media may involves the risk of being victims of cybercrime. They like to spend their leisure period on cyberspace despite their awareness level is not up to the level of understanding the seriousness of cybercrime. Some of the users are affected by the severe effect of cybercrime like receiving threat or sexually explicit material on their social media profile or vulgar comment on their posted pictures.

From the study it is evident that after providing treatments to the experimental group the group shows some improvements in the awareness level that they are aware of the fact that

social media is a haunting ground for cybercriminals and how they operate various crimes through social media. They have kept restrictions on various social media activities. Major portions are aware of the risk of various types of cybercrime on social networking sites like accepting unknown friend request, private discussion over chat room, doing video chat. Major portion are aware of the consequences of posting their pictures and tagging them as well giving like to pictures can be used for creating duplicate profile, hacking system to misuse their data or stored information into the system, displaying their present location can lead to cyber stalking and clicking on the suspicious link may spread virus or malware into the system etc. The users have become aware of protecting valuable data and other personal information stored into computer by locking the system with strong password.

Awareness about keeping the computer system protected from cybercrimes like hacking, virus affect, data misuse, spoofing and phishing etc. the system need to be protected with firewall protection software, anti-virus and anti-malware software and these software need to be updated. Avoiding the use of public wi-fi to connect to the internet, downloading software and movies from torrents to stay protected from hacking or phishing.

In reference to the **fourth objective,** the concept of cybercrime arose after multiplying the number of internet users and social media users across the world. It is the case of identifying the factors and threats which actually can cause major problems of cybercrime. Social media is recognized as the integral part of life for major part of the internet users. Almost every internet users plugged in to one or more account of social media platform. Thus the growing dependency of the users on the information and communication technology raises the risk factors and threats on social media. The following threats have been verified as identity theft, hacking, phishing and e-mail spoofing, fraud, cyber bullying, spyware, malware, intellectual property theft and stealing personal information.

In social media some more factors are responsible for making the platform for cybercrime. Factors of cybercrime are:

1. **Psychological Factor:** Users mostly do not registered cybercrime complain out of fear of spoiling their reputation. Morphing, harassment, posting sexually explicit material and vulgar comments are the major reasons for causing psychological harm to the users.

2. **Risk Factor:** The risk of being a victim of cybercrime involves various personal and environmental characteristics. Spending several hours in social media can lead impulsive people at risk to fall victims to one of these cybercrimes. It includes:

A. **Posting pictures with details:** They are not aware of the fact that deleted pictures can also be recovered and is one of the cause of cybercrime like morphing, extortion or identity theft.

B. **Sharing the locations:** It involves the risk of cyber stalking. People can easily trace a person using GPS in social media.

C. **Furnishing personal details on social media:** People can use personal details to create fake identity to perform various anti2-social and illegal activities.

D. **Tagging photos with others:** They keep on tagging their pictures with other person. Tagged pictures can be seen by all the people attached to the person who post it and also the people attached to the tagged person.

E. **Accepting unknown friend requests:** It involves the risk of adding a cyber-criminal to their social media account.

F. **Chatting with strangers:** Strangers can lure the user to reveal personal details, attracts them to meet physically. Harassment, cyber bullying, psychological & physical harm, leaking personal information are the risk associated with chatting with unknown person.

G. **Using public wi-fi:** Public wi-fi involves the risk of spreading malware, phishing, hacking, DoS attack.

3. **Economic Factor**: Cybercrime is a process where criminal put very low investment and incurred high amount of financial benefit.

In reference to the **first research question,** it is observed that the primary objective of social media is sharing of personal and profession details which leads to virtual treasure of readily accessible information. These factors made social media an easily accessible platform for cyber criminals. Online predators can easily create fake identity on social media and attack

directly with advance phishing techniques. Applications / links shared in the social media attracts users to visit those links and share their personal information. The cybercriminal using those information attacks the innocent users. Cyber-criminals use advance and sophisticated techniques / malware tools to extract information stored in social media and may perform illegal activities such as theft, fraud, extortion and intellectual property theft. The researchers prime target was female users are in this research it is observed that pornography, extortion, morphing, cyber harassment, defamation, e-mail threat, cyber stalking, sending obscene content and sexually explicit materials are the crimes where women users become most frequent victims as compared to men.

Cybercrimes attempt to strike the internet users by attacking through their electronic identity. Sophisticated malware tools are used to steal sensitive personal data from social media, credit card information stored on the shopping websites to create a fake account in social media to attack on their personal level as well as on their property. Theft, fraud, extortion and intellectual property theft or piracy are the biggest examples of cybercrimes against property. Child pornography, extortion, morphing, cyber harassment, defamation, e-mail threat, cyber stalking, sending obscene content and sexually explicit materials are the crimes where women and minors become most frequent victims as compared to men. They generally get attracted by the hoax messages and fake identities in social media and become victims to the online offenders.

The **second research question** was consequences of cybercrime. Female users are emotional in nature and can be easily convinced. Any individual or group of people can easily approach to female user and victimize them for personal benefit or benefit of large identity. Cybercrime causes identity theft & fraud, posting of sexually explicit materials & vulgar comment on social media profile causes reputation harm, cyber bullying & leaking personal information cause psychological harm arises due to private discussion over chat, cyber stalking caused due to displaying present location through GPS system, spreading malware causes damages to the system & important data, information theft caused due to the illegal access to computer system, denial of services attack causes disruption of computer system, clicking on suspicious links & spam mails causes hacking & spreading virus, misrepresentation by

spoofing and phishing technique causes data theft arises with the usage of torrents and public wi-fi.

Cybercrime is a collective effort of the advancement of digital technologies. Therefore, multidirectional approach from the law enforcement agencies, information technology industry, public private collaborations and information security organizations are essential to come up together to upgrade their skills on such technologies and find out a way to minimize cybercrime. Apart from such collaboration individuals also need to be cautious about the cyber-criminal activities on social media. To tackle down the crime, the users of social media need to be more conscious while posting and sharing anything on it so as to minimize the chance of being victimized of this crime.

Restrictions are imposed on profile privacy setting to protect from identity theft & fraud, in response to sexually explicit materials on social media profile the users used to delete or report spam or alert others or block the user, in response to vulgar comment they used to delete the comment or block the user or report abuse or ignore the user, they install and update anti-virus software to protect system against spreading malware & data loss, computer system is protected by strong password to restrict illegal access, they have knowledge about the effect on clicking on suspicious link and spam mails, they protect their social media profile by keeping restriction on their online profile to avoid leaking of personal information, they skip tagging others, skip sharing pictures, restriction imposed on the chat and video chat circle, avoid using torrents and stopped using public wi-fi to keep them secure online.

In reference to the **third research question,** there is a correlation between user's involvement and cybercrime victimization. Ignorance of the user about cybercrime and its affect can make cybercrime to operate on a much larger scale. With or without the knowledge of the regulations of the medium they enter into cyber space. Almost all the internet users create accounts in social media. Social media successfully attracts its users with its online activities. Once they stepped into cyber space they get addicted to its various applications and cannot head to move out of the space. Social media itself have some safety features that should be checked in before using any application. The present study reveals that some portions of the social media users keep their social media profile "public" and share personal information,

pictures and videos. They tag other members to their pictures, post own pictures in the display of social media profile, never update anti-virus, access public wi-fi and download software and movies from torrents. They are not fully aware of the negative effect of these activities. Such activities can make them cybercrime victims.

In reference to the **fourth research question, s**ocial media serves both personal and professional purpose. Many users put all their personal information in social media, credit or debit card details are also furnished and stored in the shopping websites for future use and purchase through social media. But it too has some loopholes like every other medium that one cannot ascertain before getting trapped into one of these loopholes. Security is one of the most important issue which directly comes under the impact of cybercrime on social media. Female users of social media mostly become the target of cyber criminals as compared to male users for many reasons though both the end users are well educated and knows the operation of digital media. The research shows that, major portion of the users from both the groups initially were not aware of the impact of cybercrime. But after providing treatments to the experimental group for the period of six months it is observed that, this group shows progress in their awareness levels. They realized the fact that social media is a platform for committing various types of cybercrimes. Social media is a virtual space where many users face many trouble with their privacy, social identity and even with their personal property. Whereas the control group shows moderate progression in their level of awareness.

Restrictions are imposed on profile privacy setting to protect identity theft and profile duplicity and strong password setting to protect computer. They have installed and update anti-virus and firewall protection software into their system. They do not keep their personal information in their social media profile. They have become skeptical while accepting friend request from any unknown person. Chat room conversation is restricted to friends and family only. They do not entertain any obscene content and derogatory comment in their profile and report back to the safety team. They become conscious on clicking any suspicious attachment or link.

In reference to the **fifth research question,** social media usage among female users is a growing trend and is proved to be helpful in the study and maintaining connectivity. Awareness measures can combat cybercrimes in various ways. The threat of cyber-attack can be marginalized by being cautious while using social media. Technology is getting advanced to move forward and makes life easier. In the same pitch cyber criminals are creating fast developing technique to abuse technology for their benefit. Not a single individual in the cyber space is protected even the government or private agencies are not fall under the risk free zone. All of them need to understand the value of taking precautionary steps and awareness measures to stop cybercrime are as follows:

- Always use anti-virus, anti-firewall and internet security software and do update it.
- Never allow anyone to access to the computer system.
- Always have back-up of the valuable computer data.
- One should not share computer system with other because they can copy important data from the system to abuse the owner.
- Secure the system with anti-firewall, anti-virus and anti-spyware software to protect against malicious software attack.
- Never give personal information like computer password and login password to unknown person.
- Never click on any suspicious link. Never response to any spam.
- Always maintain privacy setting.
- Data stored in a computer should be locked with strong password.
- Never use the same password for all online accounts.

In nutshell, not a single individual is completely unaided against cybercrime. There are provisions of fine or imprisonment or both for the cyber criminals. The techno savvy legal system designed especially for dealing with cybercrime. Under cyber laws of India, many law enforcement departments have separate sections for cybercrime. These laws are the safeguards against cybercrime to make safe electronic communication and transaction. In India,

Information Technology Act-2000 and Indian Panel Code have offered legal enactment to put cyber-criminal activities down under its various sections.

Initially there was no major difference in the awareness level of both the groups. Minor difference is observed in the awareness level of the control group however, the experimental group showed a major difference after providing treatments for a period of six months. From the test statistics, the inferences can be drawn as the awareness level of the experimental group has been raised to a significant level as compared with the control group which was exposed to the surrounding only. Treatments played a pivotal role in raising the awareness level of the respondents of the experimental group.

The study can be concluded as, women do not possess sufficient knowledge about cybercrime. In most of the cases they become major target of cyber criminals. Therefore some precautionary steps need to be followed to reduce the crime to a marginal limit while using social media. The steps include awareness about social media and cybercrime, staying alert while using social media and making others aware of the associated risk.

Suggestions:

It is important to have knowledge about social media when someone is using it. Complete and correct information about social media can save people from its adverse effect. Knowledge about social media is very important for a user. Before using such technologies complete information and understanding of the technology are required for every user so that they would have some idea of what can be the negative impact of social media activities. Cyber criminals are in search for every possible loop holes and once they found any of the loops they use it for their benefit. It is also equally important to stay alert while using such technologies. This basic knowledge can help a user from becoming a target of cyber criminals. Many people use social media without any knowledge about its various applications. Cyber criminals take the ignorance of the users to their advantage and make them target as their next cybercrime victim. Some precautionary steps should be followed to reduce the extent of cybercrime which are as follows:

Awareness: Awareness is the primary step to protect against cybercrime. Knowledge about cybercrimes and its various types can make people to stay alert about its risk. People do not have sufficient knowledge about cybercrime and its various impact. Cyber criminals take advantage of this lack of knowledge and modulate them so as to fulfill their ill motives. Technology is developing very fast and its associated crimes also growing at the same rate. So the updated information about these latest technologies can give protection against cybercrime.

Use of anti-firewall, anti-virus, anti-spyware and spam blocking software: Firewalls monitor the traffic between the computer system or network and the internet. It serves the basis for detecting the intruders and keeps them out by making a defense system. Use of the firewall software that comes up with security software and wireless network router. Spam blocking software enables the system to detect and block the unwanted bulk mails that may cause harm to the computer system. Do not respond to mails send from any unknown sources. It may be the trick to leak information or spread virus.

Use of security software and keep the system updated: Cyber criminals have multiple ways to get into the system and so the necessity arises to keep the system updated and

protected by anti-virus. Anti-virus protects the computer system against virus, worms other similar attacks. It detects and deletes the threats that come from inserting CDs/DVDs, downloading software, visiting some websites, pop-up. Software security center available in the market can protect the system from malware, phishing, spyware and from other threats. Security software needs to be updated and system scan should be performed on regular basis. Automatic update of operating system and browser should also be done.

Practice of safe online transactions: Online transactions always enquire about the safe websites. People need to be careful while shopping online and a careful investigation about the websites is necessary before making online payment. Always check for the safety and security policy about ones' personal information.

Be cautious to click: While surfing on the internet or chatting through instant messenger or checking e-mails, always have to be careful before clicking on any suspicious link or unknown link that may connect the user to a fake websites where people are asked to share their personal information like user name and password to visit the website. Clicking on any suspicious link may download malware to the system used. Some kind of viruses spread through e-mails. So it is important to be cautious before clicking any link.

To secure the wireless network: Data transmission on an unsecured wireless network can provide an opportunity to the hackers to access data or information. Enabling system security software and changing the router's administrator password people can keep away the hackers from their network. Because criminals might have the knowledge of default password and they can make use of them to hack into the network.

Use of strong password: Strong password can secure one's information from being hacked. Using passwords of at least 10 characters composed of a combination of letters, numbers and special characters. Periodical change of password reduced the likelihood of being hacked.

Use of common sense: Even if all those attempts are being made to protect against cybercrime minor mistakes can major problems. Responding to spam and downloading material from unknown or unauthorized sites are common mistakes that people make offering

the cyber criminals to perform their job easily. Posting of personal information in the social networking sites is a serious mistake people often made. So the use of common sense while surfing on the internet protects from several damages.

As per the advisory on cybercrime prevention and control[104]of ministry of home affairs there are different types of cybercrime cases are starting from vandalism of Government website, online financial frauds, online stalking/harassment, data theft or domain theft etc. cybercrime has emerged as major challenge for the law enforcement agencies. Specialized investigation techniques and forensic tools are required to combat such crimes. Cases of cybercrime involves technical, administrative and legal challenges in the investigation. It becomes necessary to upgrade institutional mechanism to combat cybercrime and therefore suggested the following steps:

1. **Institutional Setup**

i. State Cybercrime Coordination Cell: Senior Officer of ADGP or IG rank is designated as State Cybercrime Coordinator to setup units in each State or UTs. The responsibility of this cell is to setup institutional mechanism to handle cybercrime at District or police station level, to guide and facilitate officers of this unit, supervise capacity level, to provide necessary lab assets, to investigate specific cybercrime cases and making coordination with State Cybercrime Coordinators of other States to those offences comes under IT Act, 2000 that goes under the jurisdiction of multiple States. Police officers of varied designations and domain experts from the field of cyber security should be the member of the cell.

ii. District Cybercrime Cells: It may be setup as per the requirement. Deputy SP or Additional SP assisted by Sub Inspector or Inspector as considered necessary and

[104] Government of India/Bharat Sarkar. *Advisory on Cybercrime prevention and control.*Ministry of Home Affairs/Griha Mantralaya, CIS-II/CIC Division, F.No. 25017/07/2017-PM.III/CIS-II, Dated 13.01.2018. Retrieved 11 April, 2018 from https://mha.gov.in/sites/default/files/CyberCrimeprevention_15012018_0.PDF

minimum three domain experts from the field of information technology, mobile telephony, digital forensics and cyber laws are required. The head of this cell should report to the District SP but pursue complete guidance from the State Cybercrime Coordinator Cell.

2. **Cybercrime Cases Involving Inter-State or International Cooperation: S**trengthening inter-state and international cooperation mechanism is important. Steps may be taken in this regards are as follows:

i. Specific cases which involves of inter-state or international ramifications may be referred to CBI, the nodal point for Interpol.

ii. For it is required to strengthen inter-state coordination through joint investigation teams, sharing of evidences and other information which is appropriate for the fast clearance of cybercrime cases having involvement of inter-state ramifications.

3. **Cyber Forensic Labs:** It is essential to create suitable cyber forensic facility at the State or District level to investigate such cases. In this regard States or UTs may take some following steps:

i. To setup cyber forensic training lab cum training center for their officials in each State or UTs, Ministry of Home Affairs has released Rs. 82.8 crore to States or UTs under CCPWC Scheme.

ii. States or UTs may consider the setup of cloud based high tech cyber forensic labs for the efficient utilization of expensive materials

iii. Setting up of primary cyber forensic labs at District level as per the requirement.

iv. Mobile cyber forensic lab facility may be explored to reach wider area and maximum use of materials.

4. **Capacity Building:** Expert knowledge and suitable training of police officers, public prosecutors and judicial officers are required for accurate investigation and prosecution of the cases of cybercrimes and also to assists cybercrime victims.

5. **Cybercrime Prevention:** Law enforcement agencies are following the foot patrolling in colonies, keeping eyes on vulnerable localities, suspects for intelligence crowd and prevention of physical crimes.

6. **Research and Development:** To control the emerging challenges arising due to fast developing technologies, Ministry of Home Affairs plans to start R&D in cyber space. In this context, all States and UTs are advised to:

   i. Identify the requirements of R&D in certain specified areas of cyber space and update MHA regularly about such requirements.

   ii. Suggestions for the improvements in legal and policy structure may also be informed to MHA.

7. **Online Cybercrime Reporting Portal:** For online filling of complaints related to cybercrimes, Supreme Court has directed to MHA to create such platform. Accordingly MHA is creating a portal cyberpolice.gov.in, where victims can directly file complaints related to cybercrime easily.

8. **Awareness Drive:** It has been observed that due to lack of awareness about modus operandi of cyber criminals, several people are getting victimized about various types of cybercrimes. Proper education for the people through appropriate awareness campaign will help in combating such crimes to a significant extent. States or UTs may start the following steps:

   i. Regular awareness campaign to advice people for not sharing their personal credentials like user ID, password, ATM or Credit card PIN, OTP etc. Financial institution, NGOs and educational institutions may help in spreading such massages.

   ii. Awareness focused on educating the users of cyber space about various media to file cyber complaints.

iii. Awareness made to the citizens of their duty to inform about the misuse of cyberspace to the law enforcement agencies especially if the observe child pornography, obscene materials or content on social media or alike platforms.

iv. MHA is designing some illustrations in print, radio and audio visual medium which will be available at their website. States or UTs can use such creations or they may create their own designs as per the requirements.

Limitations of the Study:

The researcher has confronted with various constrains during the course of study. The major short coming was the accessibility factor. The study had to proceed with the samples collected from the female users of social media from some known users. It could have been presented in a better shape provided all the female users from my Facebook account were cooperative. The evaluations of the study would yield authentic result if all sample data had been received by the researcher. In the process of collecting data through online questionnaire tool many female users have opposed. The researcher had to confront one to all users included in the sample and elaborate the whole procedure of filling up the online form to collect data from them.

Hence, in view of the researcher, the survey method has turned to be fruitful one to draw out the correct information about their knowledge on cybercrime against women. However, it was an attempt to shape a general structure to research followed on the current issue on Social Media and Cybercrime against Women. Law and Technology are dynamic in nature. Law changes with the change in society and technology also changes with the innovative ideas to serve the society for its developments. The topic is dynamic in nature and can be further explored to know the nerve and experiences of the social media users.

*****