Awareness of Safeguarding Personal Details on social media among the social work students

Dr. Amod Gurjar

Assistant Professor,

Matru Sewa Sangh Institute of Social Work,

Bajaj Nagar. Nagpur.

Abstract:

This study was conducted to examine the awareness of social work students in Nagpur regarding the security of personal information on social media. A questionnaire was used for data collection and Google Forms were used to collect data from the students. The research examined the impact of factors such as age, gender, level of education and computer literacy on awareness.

According to the research, despite some awareness about social media security, ignorance was observed regarding several important concepts. Males, MSW students, individuals early adult aged (36-41 Years) students and students with computer literacy were found to be more aware, while females, BSW students, early youth aged (17-23 Years) and students without computer literacy were comparatively less aware. It was evident that there is a need for more training and workshops, especially for the partially aware group. Educational institutions should conduct cyber security workshops and mentoring programs to increase awareness about concepts such as digital footprints, social engineering, suspicious messages, so that students can use social media more responsibly and safely.

Introduction:

In today's digital age, where our lives are intertwined with the online world, protecting our personal data has become more critical than ever. The topic of internet privacy raises important questions about how our information is collected, stored, and used.While Social media provides a digital platform for people across the world. It creates awareness amongst people to participate and share information online (Sharma, B. K., Jain, M., &Tiwari, D. 2015). Hence in the present digital age the use of social media is increasing on large scale. Social media such as Facebook, Instagram, Twitter, WhatsApp are effectively used for communication, information exchange, education and finding career opportunities. College students in particular use social media extensively. However, its widespread and unsafe use develops the possibility of many cyber crimes, fraud incidents, identity theft, cyber harassment and misuse of confidential information.

Social media security is remarkably important for student social workers as they will be working with vulnerable and disadvantaged groups in society in the future. If they are not aware of the security of their own personal information it can have adverse effects on their professional and personal lives. Students easily take cyber risks by ignoring privacy settings while sharing personal information, not using secure passwords, communicating easily with strangers and trusting fraudulent links or websites.

The NCRB publishes the data the statistical data on crimes in its publication "Crime in India". The latest report published is for the year 2022. In all over country total cyber crimesrelated 65893 cases were registered among this in Maharashtra 8249cases were registered. In 2021 it was 5562 in Maharashtra out of 52974 in country and in 2020 it was 5496in Maharashtra out of

50035 in country. This clearly indicates year by year there is huge growth in the cases being registered at national as well as at state level. This creates the concern. In such situation Safeguarding Personal Details on social media would be tiny but most effective step towards reducing such incidences. Therefore the purpose of this research is to assess the awareness of social work students regarding the security of personal information on social media. This study will attempt to find out how much they know aboutSafeguarding Personal Details on social media. On other hand Intellectual, physical, and interpersonal competences developed throughout the college experience can be noted through using critical thinking skills, involvement, and communications. Many of these communications for college students occur through social media(Richardson, C. 2017). Hence this investigation becomes more significant in the context of the college students. In addition the social workers are change agent hence the social work students needs to be more aware than any other group as they will be involved in spreading awareness.

This research will help improve the habits of students and create more awareness among them about social media safety. The study will provide necessary recommendations and guidance to prevent cyber threats in the future, which will be of great importance for the social work sector.
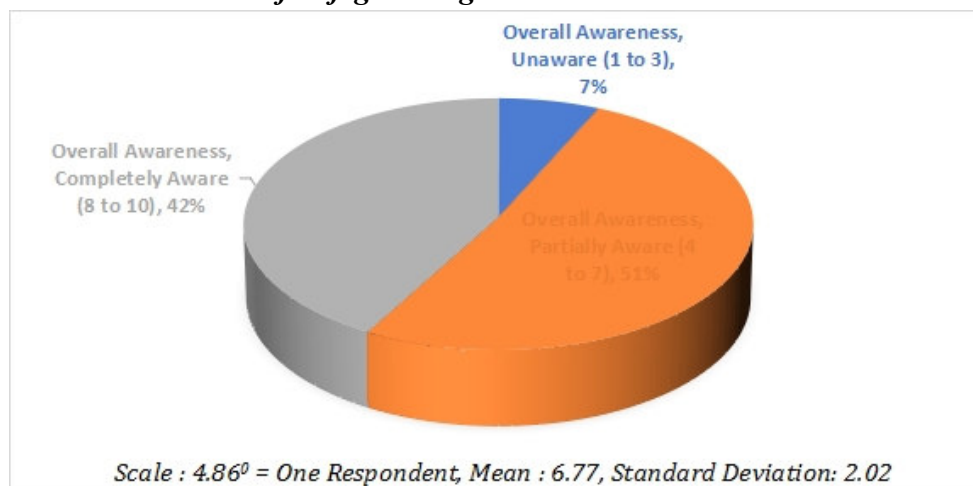
Methodology:

The study aimed at exploring the Awareness of Safeguarding Personal Details on social media among the social work students in Nagpur. For data collection the questionnaire method has been used and to collect the data from the students google form has been used. The invitation sampling method has been used for this purpose. The efforts has been made to explore the awareness and the factors like age, gender, level of education and computer literacy influencing the awareness.

Findings& Discussions:

To explore the Awareness of Safeguarding Personal Details on social media among the social work students the consolidated measurement test has been developed containing ten questions. Each question had one mark for a correctanswer, the test was of total ten marks. Overall awareness has been measured in three different categories namely Unaware (1 to 3 marks), Partially Aware (4 to 7 marks) and Aware (8 to 10 marks).

Figure 1: Overall Awareness of Safeguarding Personal Details on social media

Scale : 4.86^0 = One Respondent, Mean : 6.77, Standard Deviation: 2.02

The figure 1 reveals that, the proportion of "Unaware" students is only 7.o per cent, meaning that these students have very little knowledge about social media security and are less likely to take the necessary precautions to avoid cyber threats.The proportion of "Partially Aware" students is51.0 per cent, and this group is somewhat aware of social media security. In contrast, the proportion of "Completely Aware" students is 42.0 per cent, who are well informed about how to protect personal information on social media and follow the necessary security measures.

These findings make it clear that half (51.0 per cent) are partially aware and two out of five 42.0 per cent of students are completely aware. The average awareness score of the students in the study is 6.77 (±2.02), which falls in the category of partial awareness. Based on these findings, it can be said that there is a need to conduct more training and workshops on social media safety among the students, especially for the partial awareness group. This will increase their ability to keep their information safe and avoid cyber threats.

Table 1: Gender Influencing Overall Awareness

Gender	Overall Awareness			Total
	Unaware (1 to 3)	Partially Aware (4 to 7)	Completely Aware (8 to 10)	
Male	1	12	11	24
	4.2%	50.0%	45.8%	100.0%
Female	4	26	20	50
	8.0%	52.0%	40.0%	100.0%
Total	5	38	31	**74**
	6.8%	51.4%	41.9%	**100.0%**

Table 2: Educational Level Influencing Overall Awareness

Level of Education	Overall Awareness			Total
	Unaware (1 to 3)	Partially Aware (4 to 7)	Completely Aware (8 to 10)	
BSW	3	23	15	41
	7.3%	56.1%	36.6%	100.0%
MSW	2	15	16	33
	6.1%	45.5%	48.5%	100.0%
Total	5	38	31	**74**
	6.8%	51.4%	41.9%	**100.0%**

Table 3: Age Influencing Overall Awareness

Age	Overall Awareness			Total
	Unaware (1 to 3)	Partially Aware (4 to 7)	Aware (8 to 10)	
Early Youth Age (17 to 23)	4	30	18	52
	7.7%	57.7%	34.6%	100.0%

Middle Youth Age (24 to 29)	1	6	9	16
	6.3%	37.5%	56.3%	100.0%
Early Adult Age (36 to 41)	0	2	4	6
	.0%	33.3%	66.7%	100.0%
Total	5	38	31	74
	6.8%	51.4%	41.9%	100.0%

Table 4: Educational Level Influencing Overall Awareness

| Computer Education | Overall Awareness | | | Total |
	Unaware (1 to 3)	Partially Aware (4 to 7)	Aware (8 to 10)	
Yes	3	25	24	52
	5.8%	48.1%	46.2%	100.0%
No	2	13	7	22
	9.1%	59.1%	31.8%	100.0%
Total	5	38	31	**74**
	6.8%	51.4%	41.9%	**100.0%**

Gender and Awareness: Compared to male and female students, 45.8 per cent male students fall into the "Completely aware" group, while the proportion among female students is 40.0 per cent. This means that male students are relatively more aware of social media security. However, the proportion of males (50.0 per cent) and females (52.0 per cent) in the "partially aware" group is almost equal. Also, the proportion of female students who are "completely unaware" (8. Per cent) is higher than that of male students (4.2 percent), which means that women need more training on this topic.

Educational Level and Awareness: Compared to BSW and MSW students, 48.5 per cent of students in the MSW group are "completely aware" while the proportion in the BSW group is 36.6 per cent. This indicates that MSW students are relatively more aware. This shows that as the educational level increases, the awareness of social media safety increases. However, 56.1 per cent BSW students are more in the "partially aware" group, while the proportion is 45.5 per cent in the MSW group. This means that BSW students need more training and guidance in this regard.

Age and Awareness: By age group, 57.7 per cent of students in the Early Youth Age (17 to 23 years) are "partially aware", while only 34.6 per cent of students are "completely aware". This means that there is a need to create more awareness about safety among Early Youth Age students. The proportion of students in the Middle Youth Age (24 to 29 years) who are "Completely aware" is 56.3 per cent, which indicates that safety awareness increases with increasing age. Also, 66.7 per cent of students in the Early Adult age (36 to 41 years) are "completely aware", meaning that adults are more aware of safety and tend to take precautions.

Computer Education and Awareness: Students with computer education show greater awareness of social media safety. 46.2 per cent of students with computer education are "complete aware" compared to 31.8 per cent of students without computer education. Also, the

proportion of "partially aware" (59.1 per cent) is higher in the group without computer education, indicating that the impact of technical education on social media safety is positive.

The findings of this research show that male students, MSW level students, adults and students with computer education are more aware of social media safety. On the contrary, women, BSW students, early youth aged (17 to 23 years) and students without computer education are relatively less aware. Therefore, more training programs, workshops and guidance on safe ways to use technology are needed for these groups.

Importance of keeping personal information safe on social media: 78.4 per cent of the students have correctly understood the importance of keeping personal information safe, while 21.6 per cent of the students have answered incorrectly. Although this is a positive thing, some students still need to be educated more about social media security policies.

What information should not be shared on social media? : Greatest Majority91.9 per cent of the students answered this question correctly, which means that most of the students know that they should avoid sharing personal information on social media. However, 8.1 per cent of the students do not have a clear idea about this, which means that more emphasis needs to be placed on social media risks and prevention.

What is a digital footprint? : Only 52.7 per cent of students understood what a digital footprint is, while 47.3 per cent of students answered incorrectly. There is a need for more clarity on how a digital footprint is a track of our online transactions and how we maintain our presence in the digital world. Many still do not fully understand its meaning, so it will be important to create awareness about this in the future.

Table 5: Aspects of Awareness about Safeguarding Personal Details on social media

S.No.	Question	Wrong Answer	Correct Answer	Total
1	Why is it important to safeguard personal details on social media?(CA: To prevent identity theft and cyber fraud)	16	58	74
		21.6	78.4	100.0
2	Which of the following should NOT be shared on social media? (CA: Personal Details)	6	68	74
		8.1	91.9	100
3	What is a digital footprint? (CA: The record of all your online activities, including posts and interactions)	35	39	74
		47.3	52.7	100
4	Which of these passwords is the strongest for a social media account? (CA: P@ssW0rd!XyZ#2025)	13	61	74
		17.6	82.4	100
5	If you receive a suspicious message from a friend's social media account, what should you do? (CA: Ignore the message and report the account if necessary)	44	30	74
		59.5	40.5	100
6	What is social engineering in the context of cyber security? (CA: A trick used by cybercriminals to manipulate people into sharing sensitive information)	41	33	74
		55.4	44.6	100
7	If your social media account is hacked, what is the first step you should take? (CA: Change your	21	53	74
		28.4	71.6	100

	password and enable security measures like 2FA)			
8	Why is it risky to use the same password across multiple social media accounts? (CA: If one account is hacked, all accounts become vulnerable)	16	58	74
		21.6	78.4	100
9	What is oversharing on social media? (CA: Posting excessive personal details, making you vulnerable to cyber threats)	19	55	74
		25.7	74.3	100
10	If you receive a friend request from someone you don't know, what is the safest approach? (CA: Check their profile, mutual friends, and activity before deciding)	28	46	74
		37.8	62.2	100

Awareness of choosing a secure password: more than four fifth 82.4 per cent of students correctly identified what a secure password should be, while 17.6 per cent of students are not clear about this. Although this is a positive picture, some may still face cybersecurity threats due to the habit of keeping weak passwords.

What to do if you receive a suspicious message? : Only two fifth 40.5 per cent of students answered correctly, while almost three fifth 59.5 per cent of students responded incorrectly. This means that most students are unable to make the right decisions about suspicious messages received on social media. Many are likely to fall victim to fraud by responding to such messages. More focus is needed on this.

What is social engineering? : Social engineering is a cyber attack method in which cyber criminals use emotional or psychological pressure to obtain confidential information from people. The research showed that only 44.6 per cent of students have a proper idea of social engineering, while 55.4 per cent of students do not know its full meaning. Therefore, special training and guidance are needed to be careful of this type of cybercrime.

What should you do first if your social media account is hacked? : Nearabout three fourth 71.6 per cent of students have correctly answered that they should change their password and take additional security measures. However, remaining more than one fourth 28.4 per cent of students have answered incorrectly. This means that some students still do not have a clear idea about what to do to keep their social media accounts secure.

How dangerous is it to reuse a password? : More than three fourth 78.4 per cent of students have identified the risks that if the same password is used for multiple accounts, it can be hacked on a large scale. However, more than one fifth 21.6 per cent of students still do not have proper information about this. This shows that there is a need to create more awareness about using different strong and unique passwords for different accounts.

What is oversharing on social media? : Oversharing is sharing too much personal information on social media, which can put your safety at risk. Almost three fourth 74.3 per cent of students have a correct idea about this, while one fourth 25.7 per cent of students have answered incorrectly. This means that some students still do not fully understand the potential risks of their posts and online behavior.

What is the right action to take regarding a friend request from a stranger? : The research found that more than three fifth 62.2 per cent of students correctly answered that a friend request

from a stranger should be verified before accepting it. However, near about two fifth 37.8 per cent of students are ignorant about this, meaning that some still easily befriend strangers, which makes them more likely to fall victim to cybercrime.

Conclusion: Overall, while there is some awareness regarding social media safety, there is still ignorance regarding some important concepts. Hence it can be said that there is a need to conduct more training and workshops on social media safety among the students, especially for the partial awareness group. This will increase their ability to keep their information safe and avoid cyber threats.Study also indicates that male, MSW, Early Adult age (36 to 41 years)&Students with computer education show greater awareness of social media safety.On the contrary, women, BSW students, early youth aged (17 to 23 years) and students without computer education are relatively less aware. Therefore, more training programs, workshops and guidance on safe ways to use technology are needed for these groups.

The research also shows that while there is some awareness among students about social media safety, there is still a lack of awareness about many important concepts. While the majority of students understand the importance of keeping personal information safe, many still need to make sound decisions regarding digital footprints, social engineering, and responding to suspicious messages.

There was positive awareness about password security and the dangers of using the same password for multiple accounts, but some students were uncertain about how to take immediate measures to protect themselves from hacking. Also, there was still insufficient awareness about oversharing and contact with strangers on social media.

This clearly shows that there is a dire need for in-depth training and guidance on social media safety. With an emphasis on cyber safety workshops, digital literacy programs, and effective policies, students will be able to use social media more responsibly and safely. Therefore, educational institutions and parents need to provide students with more information about the potential dangers of social media and security measures, so that they remain safe from cybercrime.

Suggestions and Recommendations: Various measures need to be implemented to increase awareness about the security of personal information on social media. Keeping in mind the shortcomings found in the research, the following recommendations are made:

Cyber Security Workshops: Regular cyber security and digital literacy workshops should be organized in colleges, which should focus on concepts like password management, phishing attacks, social engineering.

Inclusion in the academic curriculum: Basic information about social media security should be included in the curricula, so that students become more responsible digital citizens in the future.

Awareness campaigns: Social media platforms and educational institutions should jointly conduct online and offline campaigns on safe internet use.

Emphasis on personal privacy: Students should adjust the privacy settings of their social media accounts appropriately and be careful while sharing personal information.

Promotion of safe use of technology: It is necessary to make two-factor authentication (2FA) mandatory, adopt secure password policies, and make it a habit not to respond to suspicious messages.

The implementation of these measures will enable students to use social media more safely and responsibly and avoid cyber threats.

References:

- Richardson, C. (2017). *Student perceptions of the impact of social media on college student engagement (Doctoral dissertation).* Retrieved from https://scholarcommons.sc.edu/cgi/viewcont ent.cgi?article=5444&context=etd. On 05/03/2025

- Sharma, B. K., Jain, M., & Tiwari, D. (2015). Students perception towards social media with special reference to management students of Bhopal Madhya Pradesh. International Journal of Engineering and Applied Sciences, 2(1), 30-34.Retrieved fromhttps://www.ijeas.org/download_data/IJEAS0201014.pdfOn 05/03/2025

- https://yourstory.com/2023/06/internet-privacy-safeguarding-personal-dataaccessed on 03/03/2025

- https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2003505accessed on 03/03/2025