

CYBER CRIME CHALLENGES FACED BY WORKING WOMEN IN SOCIAL MEDIA IN INDIA

Shouryasheela Prajay Patil Research Scholar Department of Law Shivaji University Kolhapur

ABSTRACT:

The incidence of cybercrime against women is rising quickly right now. The term "cybercrime" refers to a variety of crimes perpetrated online against women. The current research focused on online crimes against women committed via social media. This study has a descriptive design approach. We will survey working women in the regions of Jaipur and Ajmer who socialise online. To gather primary data, a self-designed questionnaire will be used.

Keywords – Cybercrimes, working women, challenges, Social Media

INTRODUCTION:

India is growing quickly, and one of the main drivers of this development is technical progress. You have to understand that every revolution has been for the greater good of mankind. India is unquestionably one of the most technologically advanced countries in the world, and information technology in particular. (1) Science and technology have been given a lot of attention in the concept of a modern India in order to promote inclusive development.

The drawback of this quick progress is also there. The internet users, particularly women, are more vulnerable to cybercrimes, or illicit actions committed through the internet. Women are particularly vulnerable to these online cyberattacks owing to a number of circumstances, including ignorance and a lack of privacy protections. (2) The United Nations Human Rights Council has ruled that the freedom to use the internet is now a human right. From 181.7 million users in 2015 to 216.5 million users in 2016 to a predicted 250.8 million users in 2017, the number of social network users in India has dramatically expanded. 2 By 2020, the same number is anticipated to reach at least 336.7 million. 3 According to a research on internet users in India done by the Boston Consulting Group and the Retailers Association of India, women make up around 29% of users.

It is unavoidable that women in our culture sometimes fall victim to cybercrimes, which is a serious problem given the consequences. (3) Cybercrime is a worldwide issue. With the development of technology, cybercrimes, the victimisation of women, and the objectification of women are on the rise, which presents a serious danger to one's safety and mental health. Even though India is one of the few countries to pass and execute legislation⁵ to fight cybercrimes, any particular provisions targeting the cybercrime against women are yet unaddressed. The Act has not taken into account the serious danger to women's security as a whole.

Because of the overall decline in regard for women in contemporary society and the fact that many individuals still struggle to accept the idea that merely uploading someone's photograph online constitutes a crime, cybercrimes against women are still tolerated in India. (4) Cybercrimes like email spoofing and morphing lack societal moral support and are thus treated leniently. This gets us to the most crucial point, where societal progress is required, where individuals must respect others' rights and understand what constitutes a crime.

People must learn to respect women and to refrain from interfering in other people's private lives. All of this can only be accomplished if young children are taught to appreciate women from an early age.

Therefore, in addition to stronger punitive changes, a shift in the educational system is essential to combating cybercrime against women in India. These changes need cooperation from the public, the government, NGOs, and other groups as they cannot be brought about by one section of society alone. (5)

REASONS FOR THE GROWTH OF CYBER CRIMES AGAINST WOMEN

According to the official data published by the National Crime Records Bureau, Government of India, 5752 people were detained and 9622 incidences of cybercrime were reported in 2014. 11,592 instances—a 20 percent increase in cases documented from the previous year—were reported in 2015, and 8121 people were detained.

Thus, it is abundantly obvious that with the development of information technology and widespread access to the internet, cybercrimes against women have increased in our society. And it is past time for the legislative and the administration to work closely together to stop this. (6)

The following are some of the main causes of the rise in cybercrimes against women: (7)

- The internet's limitless, ever-evolving nature;
- The affordability of the equipment.
- Several unprotected targets
- Loneliness is a major contributing factor, since many working women and staff members live far from their families and spend a lot of time on computers. As a result, the computers become their reliable friend.
- The anonymity makes it simple to hide.
- The majority of the time, cybercrimes are unreported because of social anxiety, hesitancy, shyness, and defamation fear.
- Due to the victim's hesitancy, shyness, and concern about the family's reputation in society, such cybercrimes are sometimes not even reported.

The Indian police, however, still do not always take cybercrime seriously. In such cases(8), the victimised woman or young girl should first get in touch with a women assistance cell or NGO (such as the All India Women's Conference⁷, Sakshi⁸, Navjyoti⁹, or the Centre for Cyber Victims Counseling¹⁰), which will help them and guide them through the process while also ensuring that the police do not treat any case lightly. (9) The absence of legal protection may also be seen as the primary cause of the rise in cybercrimes against women in India. Making strict rules is urgently necessary, and their correct application must also be guaranteed. It is important to hold the government and legislature responsible for taking meaningful action to safeguard women from online attacks. However, shame, mental torment, tension, and sadness make things worse. People no longer trust law enforcement because of the slow delivery of justice. It's complicated because of a lack of legal knowledge. (11) In addition, the majority of women disregard the privacy policies and guidelines posted on social networking platforms. (12) It is important to emphasise that women may contribute to the regulation of cyber-obscenity by learning about their rights and making sure to follow the safety precautions supplied and advised over the sites. Famous social media sites provide a variety of alternatives in their privacy rules to safeguard and shield women from such offenders. 13) It's also important to keep in mind that the majority of well-known websites explicitly state in their privacy policies that they will not be held liable for any harassment that users may experience at the hands of other users. Women should thus review the privacy

regulations or safety precautions associated with such offences before signing up for any other social networking site. (14) In most situations, negligence and lack of alertness are the main reasons why women are the intended victims of cyber-obscene material.

OBJECTIVES:

- To research the difficulties in working Indian women using social media encounter due to cybercrime.
- To evaluate the cybercrimes committed against working women on social media.
- To propose defences against cybercrim.

RESEARCH METHODOLOGY:

The victimisation of professional women who use social media sites like Facebook, Twitter, LinkedIn, and email is the only focus of this study. As a result, the research that is being recommended is descriptive. A study of working women using mobile or desktop internet in the districts of Jaipur and Ajmer was conducted. The sample was chosen using the convenience sampling technique. A total of 300 samples were examined. A self-designed questionnaire containing questions about social media network use patterns, reasons, difficulties encountered, etc. was utilised as the data gathering tool. Using SPSS, the gathered data were examined.

DATA ANALYSIS

Social Media Usage pattern

The respondents' preferred method of accessing social networks is through their mobile devices. Few respondents use their laptops or desktop computers to access social media networks. The majority of respondents use social networks to interact with their friends, but some also use them to publish or download documents including music, photos, videos, or podcasts. The majority of respondents (50%) use Facebook, whereas 20% use Twitter, 15% use Instagram, 10% use Whatsapp, and fewer than 5% use Google +, etc. Twitter was discovered to be the respondent's favourite social media platform. Respondents want to connect with four to five social networks at once. The majority of respondents preferred entertainment-oriented social networks over instructional network media for connecting. Just a few respondents said they preferred all societal domains, including information, entertainment, and education. The average responder spends three hours on social media, while 20% of respondents spend more than three hours on media. 60 percent of the respondents use media mostly for downloading movies, material, etc., and communicating with friends is another important reason for use. About 45% use social media to stay in touch with their pals.

Table 1: Usage Of Social Network Media

Usage of SNS	Respondents	Percentage	Total
Downloading music/video	180	60	300
Uploading music /Video	129	43	300
Posting photos	105	35	300
Blogging	60	20	300
Creating polls /quizzes	42	14	300
Chatting	174	58	300
Submitting articles to websites	48	16	300

Communication with Friends/ teachers /class fellows	135	45	300
--	-----	----	-----

Security measures awareness

The respondents' preferred method of accessing social networks is through their mobile devices. Few respondents use their laptops or desktop computers to access social media networks. The majority of respondents use social networks to interact with their friends, but some also use them to publish or download documents including music, photos, videos, or podcasts. The majority of respondents (50%) use Facebook, whereas 20% use Twitter, 15% use Instagram, 10% use Whatsapp, and fewer than 5% use Google +, etc. Twitter was discovered to be the respondent's favourite social media platform. Respondents want to connect with four to five social networks at once. The majority of respondents preferred entertainment-oriented social networks over instructional network media for connecting. Just a few respondents said they preferred all societal domains, including information, entertainment, and education. The average responder spends three hours on social media, while 20% of respondents spend more than three hours on media. 60 percent of the respondents use media mostly for downloading movies, material, etc., and communicating with friends is another important reason for use. About 45% use social media to stay in touch with their pals.

Table 2: Security measures awareness

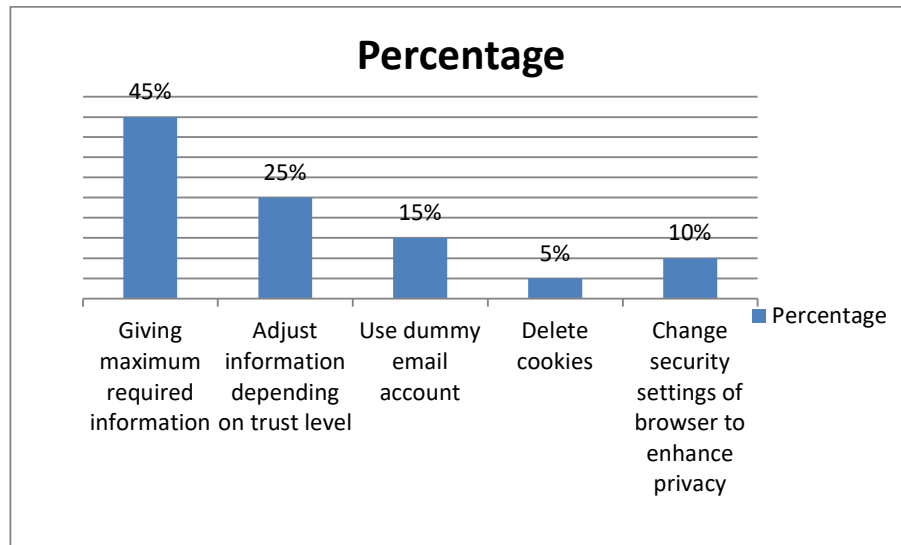
Security measures awareness	Respondents	Percentage
read the privacy policy	150	50
read the privacy policy but don't understand	105	35
ignore the privacy policy	45	15

Precaution measure

The majority of respondents said they don't accept requests from strangers. They only accept friend requests from friends of friends after carefully reviewing the requester's profile. The majority of them think it's dangerous for women to use the internet. When the respondents were questioned about their use of private policy and security settings, it was discovered that they control the display of their profiles by altering the social networking sites' basic privacy settings. Few members also trust the default privacy settings of social networking sites to secure their information. They also think it is simple to modify the default setting of their personal profile. The majority of respondents are unconcerned with social media platforms watching and documenting their users' activities. Another significant portion of respondents agree that social networking sites provide free services while earning money by selling users' personal information to marketers for customised commercial adverts.

Table 3: Protection of identity in social network sites

Statement	Respondents	Percentage
Giving maximum required information	135	45
Adjust information depending on trust level	75	25
Use dummy email account	45	15
Delete cookies	15	5
Change security settings of browser to enhance privacy	30	10

**Figure 1: Protection of identity in social network sites****Cyber Crimes faced**

When the respondents were asked whether they face any challenges while using social network site about 65% of the respondent stated that they are facing the challenges. They were asked to explain the nature challenges it was clear that 60% sometimes experience the profile hacking i.e. unable to log in to their account, 55% very rarely face challenge like Photo morphing i.e. using their images, morphing for financial/sexual gains, 45% Sometime experience Romance & dating scam, Most often every one face challenges with Offers i.e. Click on the link for gain, 35% rarely face, 55% of the them experience sometime challenges like Link Baiting i.e. content of their website or pages gets linked to other sites, Very rarely 50% of them experienced information theft of password/bank details, Often 65% of them experience Cyber bullying i.e. Posting sending vulgar message, Most often girls face challenges like Trolling i.e. Spread conflict opinions in the social network sites. The respondents were asked about the remedial action taken during such situations, most of them expressed that they will block the respective person or group, 40% stated that they will ignore the situation; another 40% also stated that they will warn them. Few of them report to the cyber crimes about the incidents.

	Often		Sometime		Rarely	
Challenges	Respondents	Percentage	Respondents	Percentage	Respondents	Percentage
Profile Hacking	90	30	180	60	30	10
Photo Morphing	45	15	90	30	165	55
Offers	255	85	30	10	15	5
Romance & Dating Scam	15	5	135	45	150	50
Link Baiting	30	10	165	55	105	35

Information Theft	120	40	30	10	150	50
Cyber bullying	195	65	60	20	45	15

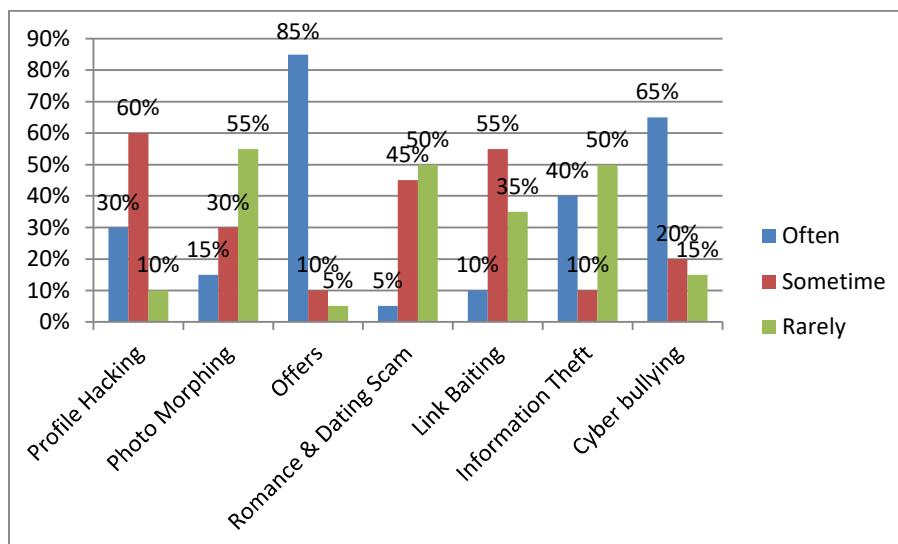


Figure 2: Challenges experienced in social network sites

Negative impact of Social Media

The negative impacts of social media on working women are--

- Cyber bullying.
- Depression.
- Lower self-esteem.
- Sleep deprivation.
- Poor concentration.
- Social isolation.
- Internet addiction
- Decreased activity

CONCLUSION:

We may conclude that cybercrime against women is on the rise on the basis of the data we have gathered. The reasons of cybercrime are many and varied. Understanding the effects on society requires understanding a variety of viewpoints.

REFERENCES:

1. Cham, 2017. Melander, Lisa A. "College students' perceptions of intimate partner cyber harassment." *Cyberpsychology, behavior, and social networking* 13.3 (2010): 263-268.
2. Saha, Tanaya, and Akancha Srivastava. "Indian women at risk in the cyber space: a conceptual model of reasons of victimization." *International Journal of Cyber Criminology* 8.1 (2014): 57.
3. Cyber law of India. Online available [www.cyberlawsindia.net/]
4. Halder D., & Jaishankar, K. (2009). Cyber Socialising and Victimisation of Women. *TEMIDA: Journal on Victimisation, Human Rights and Gender*, 12, 5-26 (September 2009).
5. Halder, Debarati, and Jaishankar Karuppannan. "Cyber socializing and victimization of women." (2009).
6. Marcum, Catherine D., et al. "Battle of the sexes: An examination of male and female cyber bullying." *International Journal of Cyber Criminology* 6.1 (2012): 904.

7. Sharma, S.K. (2013). Tumhari Sakhi. New Delhi: Bukaholic Publications.
8. Alam, S. S., Yeow, P. H. P., & Loo, H. S. (2011). An Empirical Study on Online Social Networks Sites Usage: Online Dating Sites Perspective. International Journal of Business and Management, 6(6), 155-161.
9. Thapa, Anju, and Raj Kumar. "Cyber stalking: crime and challenge at the cyber space." An International Journal of Engineering Sciences 4 (2011): 340-354.
10. Halder D., & Jaishankar, K. (2011). Cyber Gender Harassment and Secondary Victimization: A Comparative Analysis of US, UK and India. Victims and Offenders, 6(4), 386-398.
11. Avasthi, A., Kaur, R., Prakash, O., Banerjee, A., Kumar, L., & Kulhara, P. (2008). Sexual Behavior of Married Young Women: A Preliminary Study from North India. Indian Journal of Community Medicine, 33(3), 163-167.
12. Norton. (2015). Norton Cybersecurity Insights Report. Accessed on March 20, 2018 from online Available [<https://us.norton.com/norton-cybersecurity-insights-report-india>]
13. Sankhwar, Shweta, et al. "A Novel Anti-phishing Effectiveness Evaluator Model." International Conference on Information and Communication Technology for Intelligent Systems. Springer, Henry, Nicola, and Anastasia Powell. "Beyond the „sext”: Technology-facilitated sexual violence and harassment against adult women." Australian & New Zealand Journal of Criminology 48.1 (2015): 104-118.
14. National Crime Records Bureau (NCRB) of India-2016