RCHUB: JOURNAL OF CONTEMPORARY TRENDS IN MANAGEMENT, COMMERCE AND ECONOMICS (JCMCE) VOLUME 2, SPECIAL ISSUE 1, 2026
RCHUB PUBLISHER
ISSN: 3108-3501
DOI: https://doi.org/10.65725/JCMCE/2S1/006

CYBER SAFETY AND DIGITAL WELL -BEING FOR WOMEN: ONLINE RISKS AND THEIR IMPACT

[1]Dr. D. Sumathi
Assistant Professor
[2]Harsheethaa.M, [3]Aarthi.M, [4]Harini.S
PG & Research Department of Commerce
[1234]Shri Shankarlal Sundarbai Shasun Jain College for Women

ABSTRACT:

Digital technology has become an important part of our daily lives and is widely used for communication, education, employment, online shopping, banking, and entertainment. While these digital platforms provide many benefits, women also face various digital safety issues such as online harassment, cyberstalking, fake profiles, financial fraud, and privacy violations. The present study aims to understand the digital safety problems faced by women, examine their awareness and knowledge about online safety practices, and study the impact of digital crimes on their mental health, social life, and work or studies. The study is based on both primary and secondary data. Primary data were collected from 100 women respondents through a structured questionnaire using Google Forms, and the data were analysed using SPSS (Statistical Package for the Social Sciences). The findings of the study highlight the importance of creating awareness about digital safety and encouraging safer online practices to ensure a secure digital environment for women.

INTRODUCTION:

The internet and smartphones have transformed women's daily lives by providing unprecedented access to communication, education, employment, financial services, and social networking. These digital platforms serve as vital resources for personal and professional growth, enabling global connectivity and skill development. However, this increased digital participation exposes women to significant online safety threats. Cyber crimes such as online harassment, cyberstalking, identity theft, cyberbullying, privacy violations, and the non-consensual misuse of personal photographs have become increasingly prevalent. Such hostile experiences inflict severe emotional stress, damage self-confidence, and create a climate of fear. Consequently, many women are discouraged from freely expressing their opinions or fully participating in online activities, effectively limiting their digital empowerment. Digital safety—the practice of protecting individuals from online threats and harmful behaviors—is crucial to mitigating these risks. While awareness of safe internet practices significantly reduces exposure to cyber threats, a substantial number of women remain unaware of how to secure their personal data or report cybercrimes to authorities. To build a secure and inclusive online environment, it is essential to evaluate current awareness levels, understand the specific digital challenges women encounter, and analyze how these crimes impact their well-being. Accordingly, this study examines the digital safety issues

RCHUB PUBLISHER
ISSN: 3108-3501
DOI: https://doi.org/10.65725/JCMCE/2S1/006

faced by women, assesses their awareness of online security measures, and evaluates the broader impact of cybercrimes on different areas of their personal and professional lives.

Meaning of the Study:

Digital Safety: The protection of individuals from online threats and cybercrimes through responsible device usage, privacy maintenance, and secure network habits.

Online Harassment: Unwanted, offensive, or threatening behavior directed at an individual via digital channels, including abusive messaging and cyberbullying.

Cyberstalking: The repeated use of electronic communication to monitor, track, threaten, or harass a victim, inducing chronic fear and anxiety.

Cyber Crime: Illegal activities executed via digital networks or computers, such as identity theft, hacking, and financial fraud.

Women's Digital Safety: Safeguarding women from gender-specific digital risks, ensuring privacy, and securing freedom from online exploitation.

Scope of the Study:

This specific research on the critical evaluation of digital safety challenges, baseline awareness levels, and practical coping mechanisms utilized by women navigating contemporary online spaces. The geographic and social scope of the investigation is intentionally concentrated within the vibrant urban and highly concentrated educational demographics of Chennai. By focusing on this specific metropolitan population, the study captures the nuanced experiences of students, working professionals, and urban residents who interact with digital interfaces daily. It deeply explores how these women recognize cyber threats, navigate systemic online vulnerabilities, and implement self-protective behavioral or legal strategies to safeguard their privacy. Consequently, the findings provide localized, highly relevant insights into the digital resilience of urban women, offering a foundational framework for targeted regional policy interventions and tailored community safety initiatives.

Need for the Study:

The rapid integration of digital technology has transformed women's lives, making online platforms essential for communication, education, employment, and social interaction. However, this increased connectivity exposes women to rising risks of cybercrime and severe online harassment. Prevalent issues such as cyberstalking, fake accounts, unsolicited messages, privacy breaches, and financial fraud heavily undermine their digital confidence and willingness to participate in online spaces. Consequently, there is an urgent need to evaluate women's current awareness of digital safety protocols and the legal remedies available to them. This study directly investigates women's cybersecurity awareness, analyzes the explicit digital hurdles they face, and examines the profound resulting impacts on their mental health, social connectivity, academic pursuits, and professional performance. Understanding these systemic vulnerabilities is paramount, as digital safety directly impacts women's fundamental freedom and confidence. Ultimately, establishing a highly secure online ecosystem is vital for encouraging women to fully leverage evolving digital opportunities without fear.

Significance of the Study:

RCHUB PUBLISHER
ISSN: 3108-3501
DOI: https://doi.org/10.65725/JCMCE/2S1/006

This study is highly significant as digital technology becomes deeply embedded in women's daily routines for education, work, communication, and entertainment. With the continuous expansion of online activities, women face an escalating risk of encountering complex cyber threats and safety violations. Investigating these distinct challenges is essential for designing and promoting a measurability secure, gender-inclusive digital environment. By evaluating women's current awareness levels and identifying prevalent online problems, this research fills a critical gap in existing empirical literature regarding the toll of digital crimes on personal and social well-being. Furthermore, the actionable data generated offers a valuable framework for educational institutions, policy architects, cybercrime authorities, and community organizations to build targeted safety initiatives. Ultimately, these insights empower women to proactively manage their digital footprints, identify hidden risks, and adopt robust internet defense practices. This comprehensive approach fosters an informed culture of widespread cybersecurity.

Reviews of Literature:

- Sharma (2025):Examined cyber violence against women legally and socially, noting that safety measures fail to keep pace with digital growth, leaving victims unaware of available legal remedies.
- Martin (2025): Analyzed the rise of AI-generated synthetic imagery and deepfakes, arguing that reactive "removal-only" frameworks fail and advocating for proactive technical barriers by developers.
- Beevi et al. (2025): Critiqued India's IT Act (2000) regarding modern identity theft, highlighting how digital sabotage is weaponized to dismantle women's professional reputations.
- Kaushik (2025): Evaluated cyberstalking impacts on women, emphasizing that social media exposure increases vulnerability and pointing to a deficit in specific legal protections.
- Addala Radha Krishna et al. (2025): Discussed the dual nature of digital transformation, which empowers female entrepreneurship while exposing them to sophisticated cyber threats due to inadequate security training.
- United Nations Geneva (2025): Highlighted the global escalation of digital violence against women, stressing the necessity of international cooperation and robust policy frameworks.
- Enock et al. (2024): Demonstrated that women experience significantly higher emotional distress and stress from online harassment compared to men, impacting their digital engagement.
- Mas'udah et al. (2024): Categorized emerging gender-based cyber violence, including "Open Booking" scams and forced pornography used to exert virtual control.
- Chadha (2024): Explored social media misuse, finding that anonymous accounts and unpunished harassment compel women to restrict their online participation.
- Torrao et al. (2024): Revealed that over 80% of surveyed women alter physical travel behaviors and avoid specific public transit apps due to prior trauma from digital or physical harassment.

Research Gap:

RCHUB PUBLISHER
ISSN: 3108-3501
DOI: https://doi.org/10.65725/JCMCE/2S1/006

While existing literature extensively explores the legal definitions of cybercrime, data privacy statutes, and isolated incidents of cyberbullying, limited research integrates women's baseline awareness, specific daily digital safety challenges, and the multi-dimensional impacts on mental health, social life, and professional duties into a cohesive analysis. This study addresses that gap by evaluating these interrelated factors collectively.

Objectives of the Study:

- To examine women's awareness and knowledge regarding online safety practices.
- To investigate the specific digital safety problems encountered by women and identify high-risk online platforms.
- To analyze the physiological, mental, social, and professional impacts of digital crimes on women.

Analysis & Interpretation (Frequency Tables):

1. Demographic & Usage Profiles (Frequency Distributions)

Interpretation:

The survey sample is heavily skewed toward young women in the 18–25 age bracket (71%), supplemented by minor representations from those below 18 (12%), 26–35 (9%), and above 35 (8%). Reflecting this age structure, students comprise the majority of the sample (63%), alongside employed professionals (28%) and homemakers (6%). The respondents exhibit high educational attainment, with 43% being postgraduates and 41% undergraduates. Geographically, the sample is predominantly urban, with 75% residing in cities and 25% in rural areas.In terms of digital behavior, mobile phones are the primary gateway to the internet for 86% of respondents. They are highly experienced users, as 63% have been online for more than 3 years, and 46% spend over 3 hours daily online. While their primary online motives are headed by education (36%), they also maintain balanced engagement across entertainment (23%), social media (21%), and work (20%).

RCHUB PUBLISHER
ISSN: 3108-3501
DOI: https://doi.org/10.65725/JCMCE/2S1/006

FEATURES	FACTORS	PERCENTAGE
Age	Below 18	12
	18-25	71
	26-35	9
	Above 35	8
Educational Qualification	School level	16
	Undergraduate	41
	Postgraduate	43
Occupation	Student	63
	Employed	28
	Homemaker	6
	Others	3
Area of residence	Rural	25
	Urban	75
Type of device mostly used to access the internet	Mobile	86
	Laptop	8
	Tablet	6
Average daily internet usage	Less than 1 hour	17
	1-3 hours	37
	More than 3 hours	46
Main purpose of internet use	Education	36
	Work	20
	Social media	21
	Entertainment	23
Year of internet usage	Less than 1 year	11
	1-3 year	26
	More than 3 years	63

2. Descriptive Mean Analysis of Study Variables

Awareness of Online Safety Practices :

The Respondents showed the highest awareness for safe interaction with unknown people (Rank 1, Mean = 2.65), keeping personal information private (Rank 2, Mean = 2.64), and the risk of sharing photos and videos (Rank 3, Mean = 2.60). They showed moderate awareness for careful social media use (Rank 4, Mean = 2.59) and the lowest awareness for public Wi-Fi caution (Rank 5, Mean = 2.37).

RCHUB PUBLISHER
ISSN: 3108-3501
DOI: https://doi.org/10.65725/JCMCE/2S1/006

Statements	Mean	Standard deviation	Ranking
Safe ways of using internet	2.51	0.541	6
Importance of keeping personal information private	2.64	0.523	2
Use social media carefully	2.59	0.514	4
Risk of sharing photos and videos online	2.60	0.550	3
Safe interaction with unknown people online	2.65	0.539	1
Responsible use of social networking sites	2.45	0.642	7
Need caution while using public Wi-Fi	2.37	0.677	8
General rules for safe online behaviour	2.53	0.594	5

Mean and Standard deviation of women's awareness and knowledge about online safety practices.

Digital Safety Problems & Platforms:

Interpretation:

The respondents identified online cheating through fake profiles as the most prominent digital safety problem (Rank 1, Mean = 4.50), closely followed by women receiving unwanted messages from strangers (Rank 2, Mean = 4.47). They ranked the creation of fake accounts to contact women online as the third most significant issue (Rank 3, Mean = 4.36). General face safety problems while using social media received a moderate ranking from the participants (Rank 4, Mean = 4.32). Conversely, respondents indicated lower relative concern for issues involving financial exploitation, ranking social media misuse for financial cheating (Rank 7, Mean = 4.17) and cyberstalking as a common problem (Rank 8, Mean = 4.14) at the bottom of the scale.

RCHUB PUBLISHER
ISSN: 3108-3501
DOI: https://doi.org/10.65725/JCMCE/2S1/006

Statements	Mean	Standard deviation	Ranking
Women face safety problems while using social media	4.32	0.875	4
Fake accounts are created to contact women online	4.36	0.746	3
Some fake accounts ask women to buy products online	4.30	0.798	5
Women lose money after trusting such online sellers	4.23	0.815	6
Online cheating happens through fake profiles	4.50	0.718	1
Social media is misused to cheat women financially	4.17	0.817	7
Women receive unwanted messages from strangers	4.47	0.758	2
Cyberstalking is a common online problem for women	4.14	0.954	8

Mean and Standard deviation of the digital safety problems faced by women and the online platforms where harassment commonly occurs.

Impact of Digital Crimes:

Interpretation:

This table ranks eight statements detailing how digital crimes impact women based on their mean agreement scores. The statement "Online problems affect women's mental health" ranks first with the highest mean score of 4.25 (SD = 0.809)."Online harassment affects self-confidence" ranks second (Mean = 4.22), closely followed by "Negative content on social media causes stress" in third place (Mean = 4.20).Continuous negativity making women feel helpless ranks fourth (Mean = 4.16), while disturbing peace of mind and affecting social life share the sixth rank (Mean = 4.14)."Too much negativity on social media may lead to suicidal thoughts" ranks lowest at eighth place with a mean score of 4.01, though it exhibits the highest standard deviation (0.948), indicating the greatest variance in participant responses.

RCHUB PUBLISHER
ISSN: 3108-3501
DOI: https://doi.org/10.65725/JCMCE/2S1/006

Statements	Mean	Standard deviation	Ranking
Online problems affect women's mental health	4.25	0.809	1
Negative content on social media causes stress	4.20	0.765	3
Online harassment affects self-confidence	4.22	0.824	2
Negative comments disturb peace of mind	4.14	0.817	6
Online issues affect women's social life	4.14	0.853	6
Online problems affect studies or work	4.11	0.852	7
Continuous negativity makes women feel helpless	4.16	0.825	4
Too much negativity on social media may lead to suicidal thoughts	4.01	0.948	8

Mean and Standard deviation of the how digital crimes affect women's mental health, social life, and work or studies.

Suggestions:

- Enhance Digital Literacy Workflows: Educational institutions and corporate workplaces must routinely host interactive workshops focusing on safe browsing habits, two-factor authentication, and privacy configuration.
- Promote Cyber Helpline Awareness: Disseminate widespread information regarding national cybercrime reporting portals (such as India's cybercrime helpline and portal) to ensure victims can seek prompt legal intervention.
- Foster Supportive Family & Social Environments: Encourage open, non-judgmental dialogues within households regarding online experiences so victims can report cyber abuse immediately without fear of social stigma.
- Institutional & Governmental Support: Non-governmental organizations and state bodies should establish specialized psychological counseling cells and legal assistance desks tailored for cybercrime survivors.

ISSN: 3108-3501
DOI: https://doi.org/10.65725/JCMCE/2S1/006

CONCLUSION:

The study concludes that while digital platforms provide essential opportunities for education, employment, and social connection, women continue to encounter pervasive digital threats, including fake profiles, cyberstalking, and financial fraud. Although respondents demonstrate moderate awareness regarding fundamental online privacy, critical vulnerabilities remain—particularly concerning public network safety and formal cyber-reporting mechanisms. Because digital crimes inflict profound damage on mental health, self-esteem, and professional productivity, a collaborative approach involving educational institutions, technology providers, legal authorities, and civil society is mandatory to build an inclusive, secure digital ecosystem.

References:

[1.] Sharma, A. (2025). Legal and social perspectives on cyber violence against women: An analysis of awareness, anonymity, and digital safety measures. "Journal of Gender-Based Violence", 9(1), 22-41.

[2.] Martin, N. (2025). Beyond the whack-a-mole: Proactive technical barriers and legal frameworks against AI-generated synthetic imagery and deepfakes. "Journal of AI Ethics and Law", 3(1), 12-29.

[3.] Beevi, J. H., et al. (2025). Bridging the legal gap: A critical analysis of India's IT Act (2000) versus modern cyber threats and identity theft. "Indian Journal of Cyber Law and Policy", 12(1), 34-50.

[4.] Kaushik, R. (2025). Cyberstalking and its impact on women's safety: Evaluating privacy settings, legal frameworks, and digital practices. "Journal of Cyber Criminology", 17(1), 55-70.

[5.] Lokesh, et al. (2025). IoT and AI integration for real-time safety applications: Smart sensors and distress signal detection. "IEEE Transactions on Technology and Society", 6(1), 80-95.

[6.] Addala Radha Krishna, K., et al. (2025). The double-edged sword of digital transformation: Balancing women's entrepreneurship and cybersecurity risks. "Journal of Digital Economy and Women's Empowerment", 14(2), 112-128.

[7.] United Nations Geneva. (2025). Global digital violence against women: International cooperation, stronger policies, and safe online environments."United Nations Publications".

[8.] Enock, F., et al. (2024). Understanding gender differences in experiences and concerns surrounding online harms: A short report on a nationally representative survey of UK adults. "Computers in Human Behavior", 153, 1-12.

[9.] Mas'udah, S., et al. (2024). Emerging forms of gender-based cyber violence: "Open Booking" scams, symbolic dominance, and virtual harassment. "Cyberpsychology, Behavior, and Social Networking", 27(8), 540-555.

[10.] Chadha, M. (2024). Social media misuse and digital risks: Understanding online harassment and the safety of women. "Media, Culture & Society", 46(5), 901-918.