

Role of Women in Digital Safety and Cyber Awareness

Dr. Manju Gupta

Professor (Jagannath University), NH-12, Chaksu Bypass, Tonk Road, Jaipur-303901, Rajasthan

DOI: <https://doi.org/10.51244/IJRSI.2026.1307000204>

Received: 22 July 2026; Accepted: 28 July 2026; Published: 07 August 2026

ABSTRACT

In the digital era, women's participation in online spaces has increased significantly, highlighting the growing importance of digital safety and cyber awareness. Digital safety refers to the protection of information, communication systems, and personal data from unauthorized access and cybercrimes, whereas cyber awareness aims to educate users about potential threats and safe online practices. Both aspects are particularly important for women, as they actively use digital platforms for education, entrepreneurship, social interaction, and e-governance services. Women face several challenges in the field of digital safety, including limited technological access, lack of digital literacy, online harassment, privacy violations, and the increasing complexity of cybercrimes. Addressing these challenges requires technical measures such as multi-factor authentication, secure password management, and data encryption, along with awareness campaigns and training programs. Governments, educational institutions, and social organizations can strengthen women's participation by implementing women-centric policies, organizing cyber safety workshops, and simplifying grievance redresser mechanisms. Women's active participation in cyber awareness campaigns not only strengthens personal safety but also contributes to the creation of a secure digital culture at the community level. Their involvement makes the digital environment more inclusive, responsible, and balanced. Therefore, women's engagement in digital safety and cyber awareness is essential for establishing a safe, empowered, and inclusive digital society.

Keywords: Role of Women, Digital, Safety, Cyber Awareness

INTRODUCTION

The rapid development of information and communication technology in India has significantly increased women's digital presence. The widespread availability of smart phones, affordable internet services, and access to digital devices have enabled women to participate actively in education, employment, entrepreneurship, healthcare services, and social networking. Through social media platforms such as Facebook, Instagram, Twitter, WhatsApp, and YouTube, women exchange ideas, access educational and professional content, and promote their businesses and enterprises. Digital education and remote working opportunities have also helped women balance domestic responsibilities with professional life, thereby enhancing their digital literacy and self-reliance.

Furthermore, e-governance services, online healthcare systems, digital payment platforms, and e-commerce applications have accelerated women's socio-economic empowerment. Women are also using digital platforms to express their voices in political and social discussions. However, a clear digital divide persists in rural areas, where women's access to the internet, digital devices, and digital literacy remains comparatively lower than that of men. Socio-cultural barriers, economic inequalities, and inadequate technological infrastructure further deepen this gap. Therefore, policy-level interventions are essential to promote equal access to digital literacy and technology so that women in both rural and urban areas can fully benefit from the digital revolution.

Definition of Digital Safety and Cyber Awareness

Digital safety and cyber awareness constitute a systematic approach through which the confidentiality, integrity, and availability of information, data, and communication systems are protected while simultaneously

enhancing users' cognitive and behavioral capacities to identify and prevent cyber risks. This includes technical measures such as encryption, firewalls, multi-factor authentication, policy frameworks, risk management, and safe online practices such as password management and avoiding suspicious links. The primary objective is to create a secure digital culture through the integration of technological, organizational, and human factors.

A. Digital Safety:-Digital safety refers to the protection of personal digital devices, internet applications, online accounts, and personal data. It includes password management, privacy settings, protection against hacking or data theft, defense against phishing and malware, and responsible online behavior. The primary purpose of digital safety is to maintain personal privacy, prevent financial loss, and ensure a secure online experience.

B. Cyber Awareness:-Cyber awareness refers to knowledge and understanding of cyber risks, online threats, and digital safety measures. It is the ability to make informed decisions in the online environment, recognize potential threats, and respond appropriately. Cyber awareness includes knowledge about social engineering, phishing, malware, cyber stalking, online bullying, and other cybercrimes. A cyber-aware woman not only protects herself but also safeguards her family and community.

Thus, digital safety forms the technological and organizational foundation of protection, while cyber awareness reduces human vulnerability. Together, they create a secure, reliable, and responsible digital environment.

OBJECTIVES AND IMPORTANCE OF DIGITAL SAFETY AND CYBER AWARENESS

The purpose of digital safety and cyber awareness is to protect users from cyber threats and promote safe online behavior. Its significance lies in safeguarding personal data, privacy, and social trust while laying the foundation for a secure, inclusive, and responsible digital society.

Objectives

1. Understanding the Current Digital Status of Women

Women's digital literacy and online presence in India are continuously increasing, yet the digital divide remains evident. Rural women have limited access to smart phones and internet services, while urban women are more active in social media and e-governance services. Lack of digital literacy often prevents women from understanding safe online practices and using technological tools effectively, making them more vulnerable to cybercrimes and fraud.

2. Identification of Cyber Risks

Women frequently encounter cyber stalking, online harassment, email spoofing, circulation of obscene content, deep fake misuse, and online banking fraud. Such crimes negatively impact mental health, social reputation, and financial security. Deep fake technologies, for instance, are increasingly used to manipulate women's images, while phishing attacks steal personal and financial information.

3. Promotion of Safety Measures

Women must be informed about personal digital safety measures such as strong password management, multi-factor authentication (MFA), secure social media privacy settings, and safe browsing practices. Avoiding suspicious links and regularly updating antivirus software further strengthen digital protection.

4. Analysis of Awareness Programs

The Government of India and various organizations have initiated several campaigns to strengthen women's digital safety and empowerment. The "Digital Shakti" campaign educates women about cyber safety and online

rights, while the National Commission for Women (NCW) has introduced online complaint portals and training programs. NGOs also contribute through workshops and community awareness programs.

5. Awareness of Legal Frameworks

India has several legal provisions to address cybercrimes. The Information Technology Act, 2000 and its amendments regulate cyber offenses. Women can file complaints through the National Cyber Crime Reporting Portal, and cyber cells established in police stations investigate online harassment, fraud, and circulation of obscene content.

6. Providing Solutions and Recommendations

Practical solutions such as digital literacy campaigns, cyber safety education in schools and colleges, policy reforms, women-specific help lines, and quick grievance redressal mechanisms are essential. Promoting digital ethics and responsible online behavior is equally important for ensuring women's digital safety.

Digital safety and cyber awareness are integral to women's empowerment. They equip women with the knowledge, skills, and resources necessary to benefit fully from the digital revolution.

Women's Current Position in the Digital World

Women's digital status in India is multidimensional, involving literacy, access to digital devices, social media participation, and government initiatives. Urban women increasingly use smart phones, internet banking, and e-governance services, while rural women face limited access and training opportunities. Social media platforms such as Facebook, Instagram, WhatsApp, and YouTube are widely used by women for education, employment, entrepreneurship, and communication. Despite these advancements, the digital divide and gender inequality remain significant challenges. Rural women often lack internet connectivity, electricity, and digital devices, limiting their access to educational and economic opportunities. To address this issue, initiatives such as the "Digital Shakti" campaign, supported by the National Commission for Women, aim to strengthen cyber awareness and digital literacy among women.

Cybercrimes against Women: Types and Trends

The number and complexity of cybercrimes targeting women have increased significantly in the digital age. Major forms include online harassment, cyber stalking, and identity theft, circulation of obscene content, deep fake misuse, and financial fraud. These crimes affect women's privacy, mental health, financial stability, and social reputation.

Types of Cybercrimes

➤ Cyber stalking

Cyber stalking involves constant monitoring of a woman's online activities, repeated unwanted messages, and misuse of personal information. It creates fear and insecurity among victims.

➤ Online Harassment and Cyber bullying

Women frequently encounter abusive comments, threats, and public humiliation on social media platforms, negatively affecting their confidence and mental health.

➤ Email Spoofing and Identity Theft

Fraudulent emails resembling genuine communications are used to steal passwords, banking information, and personal data through phishing attacks.

➤ Circulation of Obscene Content and Blackmail

Unauthorized sharing of private images or videos is often used for blackmail and social humiliation.

➤ **Deep fake and Cyber Pornography**

Artificial intelligence-based deep fake technologies are increasingly misused to manipulate women's images and damage their reputations.

➤ **OTP and Online Banking Fraud**

Fraudsters manipulate victims into revealing OTPs or clicking phishing links, resulting in financial losses and psychological distress.

These crimes discourage women from participating actively in digital spaces and hinder their empowerment. Strong legal measures and awareness programs are therefore essential.

Active Role of Women in Digital Safety

Women today are not only digital consumers but also active contributors to digital safety and cyber awareness initiatives. Through awareness campaigns, safe online practices, and peer education, women play a significant role in creating a secure digital environment.

Key Areas of Participation

❖ **Personal Digital Safety Practices**

Women can protect themselves by using strong passwords, enabling privacy settings, and adopting multi-factor authentication (MFA).

❖ **Safe Social Media Practices**

Avoiding unknown contacts, limiting the sharing of personal information, and reporting abusive behavior are essential practices for online safety.

❖ **Peer Education and Community Awareness**

Women can educate other women about cyber safety through community discussions, workshops, and social media awareness campaigns.

❖ **Contribution of Women Educators and Leaders**

Women educators, social activists, and leaders organize workshops, awareness programs, and digital literacy training sessions to promote cyber safety.

❖ **Expansion of Digital Literacy Programs**

Community centers, NGOs, and self-help groups can provide women with training in internet usage, online banking, and cybercrime prevention.

Women's active participation strengthens not only personal security but also the collective digital culture of society.

Initiatives and Programs for Cyber Awareness

Several initiatives and programs have been launched to strengthen cyber awareness among women and citizens in general.

➤ **Digital Shakti Campaign**

The Digital Shakti campaign, launched by the Government of India in collaboration with the National Commission for Women, has trained over three lakh women in digital literacy and cyber safety. It focuses particularly on rural and marginalized communities.

➤ **NCW Recommendations**

The National Commission for Women has published a report containing over 200 recommendations related to women's digital safety, legal reforms, awareness programs, and cybercrime reporting mechanisms.

➤ **Shakti Suraksha Initiative**

This initiative educates women about safe online practices, social media safety, and cybercrime prevention through workshops and online awareness programs.

➤ **Cyber Safety Education in Schools and Colleges**

Educational institutions are increasingly integrating cyber safety and digital literacy into their curricula to prepare young women for secure digital participation.

➤ **Rural Awareness Campaigns**

Special campaigns in rural areas focus on internet access, Smartphone usage, online banking, and safe digital behavior through local language training programs.

These initiatives contribute significantly to creating a secure and responsible digital society.

Legal Framework and Complaint Mechanisms

India has established several legal provisions and complaint mechanisms to protect women from cybercrimes.

I. Cyber Laws and Women's Protection

The Information Technology Act, 2000 and relevant sections of the Indian Penal Code (IPC), including Sections 354D, 499, and 509, provide protection against cyber stalking, online harassment, and misuse of personal information.

ii. National Cyber Crime Reporting Portal

Women can register complaints related to cyber stalking, online fraud, obscene content, and identity theft through the National Cyber Crime Reporting Portal.

iii. Women Helpline 181 and Emergency Number 112

These help lines provide legal guidance, counseling, and emergency support for women facing cyber harassment or violence.

iv. Anonymous Complaint Facility

Women can register anonymous complaints without disclosing their identity, reducing fear of social stigma and retaliation.

v. Legal and Psychological Support

Government agencies, NGOs, and counseling services provide legal assistance, mental health support, and rehabilitation resources for cybercrime victims.

A strong legal framework and effective complaint mechanisms are essential for ensuring a secure digital environment for women.

Challenges Faced by Women in Digital Safety and Cyber Awareness

Women encounter multiple challenges in achieving digital safety and cyber awareness. These include lack of digital literacy, limited internet access in rural areas, social stigma, lack of privacy awareness, inadequate technical support, and limited access to training resources.

Such barriers restrict women's digital participation and confidence, thereby slowing the process of digital inclusion.

Solutions for Women's Digital Safety and Cyber Awareness

Several measures can strengthen women's digital security and empowerment:

1. Women-centric digital literacy programs
2. Improved rural internet connectivity and affordable digital devices
3. Stronger social media safety features
4. Mandatory cyber safety education in schools and colleges
5. Women-specific legal and psychological support services
6. Community-based awareness networks
7. Expansion of digital training and assistance centers
8. Policy reforms and stronger governmental support

These solutions collectively contribute to a secure, inclusive, and empowered digital society.

FUTURE DIRECTIONS AND CONCLUSION

In the age of artificial intelligence and emerging technologies, women's digital safety must become a top priority. As cyber threats continue to evolve, technical safeguards alone are insufficient; women must also be empowered through digital literacy and cyber awareness. AI-based tools such as automated threat detection systems, harmful content moderation, and rapid grievance redressal mechanisms can significantly enhance women's safety online. At the policy level, stronger cyber laws, effective implementation of recommendations made by the National Commission for Women, increased budget allocations for digital literacy programs, and coordinated efforts among governments, educational institutions, families, and communities are essential.

Ultimately, "Digital Safety Begins with You." Women's awareness, vigilance, and active participation are the foundations of a secure digital society. By adopting safe online practices, protecting personal information, and reporting cybercrimes promptly, women can not only protect themselves but also inspire others to participate confidently and safely in the digital world.

POSSIBLE RESEARCH QUESTIONS

1. How can women's digital safety be strengthened in the era of artificial intelligence and emerging technologies?
2. What is the current status of digital literacy programs for women in India, and where are improvements needed?
3. How does the lack of internet access and digital devices in rural areas affect women's digital safety?
4. What challenges arise in implementing women-specific safety features on social media platforms?
5. How can mandatory cyber safety education in educational institutions improve women's security?
6. How effective are current legal and psychological support systems for women affected by cybercrimes?
7. How can community networks and self-help groups contribute to spreading cyber awareness among women?
8. How can technical training and support centers strengthen women's digital empowerment?
9. To what extent can policy reforms and governmental support ensure women's digital security?
10. What is the significance of the statement "Digital Safety Begins with You" in relation to women's awareness and active participation?

REFERENCES

1. Sharma, R. (2021). *Women's Digital Literacy and Cybercrime: An Analytical Study*. Journal of Educational Research, 8(2), 45–60.
2. Data Security Council of India (DSCI). (2023). *Cyber Security Guidelines*. New Delhi: DSCI Publications.
3. Information Security Education and Awareness (ISEA). (2023). *Infosec Awareness Guidelines*. Hyderabad: IIIT.

4. Singh, P., & Verma, S. (2023). *Artificial Intelligence and Women's Safety: A Sociological Perspective*. Indian Sociological Review, 17(1), 88–104.
5. National Commission for Women (NCW). (2024). *Report and Recommendations on Women's Digital Safety*. New Delhi: NCW Publications.
6. Singh, P., & Verma, S. (2024). *Cybercrime and Women's Safety: A Sociological Perspective*. Indian Sociological Review, 18(2), 101–118.
7. Press Information Bureau (PIB). (2025). *Gyan Bharatam Mission: Digitization and Preservation of Manuscripts*. Government of India, New Delhi.
8. Sharma, R. (2025). *Digital Literacy and Women's Safety: An Analytical Study*. Journal of Educational Sciences, 12(3), 45–62.
9. Gupta, A. (2025). *Digital Education and Gender Equality: An Indian Perspective*. Higher Education Research Journal, 13(3), 101–120.
10. UNESCO. (2025). *Global Report on Digital Education and Gender Equality*. Paris: UNESCO Publications.
11. YouTube. (2025). *Digital Safety Awareness Video Series*. Retrieved from: <https://www.youtube.com/>