



Protecting Women from Cyber Risks: Challenges and Practical Solutions

Dr. V. Rohini Kumari

Lecturer in Statistics, SG Government Degree College, Piler.

Abstract: The increasing use of digital technology has created new opportunities for women in education, employment, and social networking. At the same time, it has increased exposure to online threats such as cyber harassment, digital fraud, stalking, and misuse of personal information. These risks negatively affect women's safety, mental well-being, and participation in digital spaces. This paper examines major cyber risks faced by women and proposes effective solutions involving legal protection, technological tools, education, and social awareness to promote a safer digital environment.

Keywords: Cyber security, women safety, cybercrime, online harassment, digital privacy

Introduction

The digital world has become an inseparable part of everyday life. Women increasingly use online platforms for education, professional development, entrepreneurship, and communication. However, the digital environment is not always secure. Many women experience abuse, threats, and exploitation through online platforms. These challenges not only affect individuals but also restrict women's freedom, confidence, and equal participation in digital spaces. Therefore, ensuring cyber safety for women has become a critical global concern

Common Cyber Risks Experienced by Women

1. Online Abuse and Hate Speech:

Online abuse and hate speech have emerged as major concerns for women in digital environments. Women who use social media, discussion forums, or professional networking platforms often encounter offensive messages, insulting comments, threats, and deliberate attacks. These forms of harassment may involve sexist language, defamation, body shaming, and even threats of physical or sexual harm. Women who express opinions on social, political, or professional matters are frequently singled out and subjected to coordinated online hostility.

The problem is often worsened by the anonymity provided by the internet. Offenders can hide behind fake identities or anonymous accounts, allowing them to spread hateful content, circulate false information, or publicly shame women without facing immediate consequences. Such actions can damage personal reputations and cause emotional suffering, including anxiety, fear, and stress. Repeated exposure to online harassment may negatively affect mental well-being, reduce self-confidence, and push women to withdraw from digital platforms.

Online abuse also restricts women's freedom of expression. To avoid harassment, many women limit their online presence or avoid sharing their views on important issues. This leads to reduced participation of women in digital discussions, especially in areas like politics, technology, and public policy. As a result, the internet fails to serve as an equal and empowering space for all users.

Combating online abuse and hate speech requires coordinated efforts at multiple levels. Effective cyber laws, strict enforcement, and accessible complaint systems can discourage offenders. Social media companies should adopt improved content moderation tools and provide simple options for reporting or blocking abusive accounts. At the same time, awareness programs and digital literacy initiatives can promote respectful online conduct and inform users about the consequences of cyber harassment. Such combined efforts can help create a safer digital environment where women can express themselves with confidence and security.

2. Digital Stalking:

Cyberstalking refers to the repeated and unwanted use of digital communication to monitor, contact, or intimidate a person. It may involve constant messaging, tracking someone's online activities, sending threatening or disturbing content, or repeatedly commenting on social media posts. In many cases, the offender closely observes the victim's online presence, gathers personal information, and uses it to harass or control them. This behavior can occur through emails, social media platforms, messaging apps, or other online channels.

Unlike one-time harassment, cyberstalking is continuous and intentional, which makes it more frightening for the victim. The repeated nature of the contact creates a sense of being constantly watched or followed, even in private digital spaces. Victims may begin to feel unsafe using the internet, checking messages, or sharing personal updates. In some situations, cyberstalks may also spread false information, impersonate the victim, or attempt to damage their reputation.

The psychological impact of cyberstalking can be severe. Victims often experience anxiety, fear, emotional distress, and loss of peace of mind. The stress caused by constant monitoring or threatening messages may affect their daily routines, work performance, and social relationships. Some individuals may withdraw from online platforms or limit their interactions to avoid further harassment.

Addressing cyberstalking requires a combination of legal action, technological safeguards, and awareness. Strong cyber laws and prompt reporting mechanisms can help protect victims and punish offenders. At the same time, individuals should be encouraged to use privacy settings, block suspicious accounts, and avoid sharing sensitive personal information online. Increased awareness and education about digital safety can play an important role in preventing cyberstalking and supporting those affected by it.

3. Misuse of Personal Information:

The misuse of personal information is a common cyber risk faced by many internet users, especially women. Offenders often collect personal data such as photographs, phone numbers, addresses, or identity details from social media accounts, public databases, or through deceptive messages. This information may be used to create fake profiles, impersonate the victim, or carry out financial fraud. In some cases, criminals use stolen data to send false messages, request money from contacts, or spread misleading content in the victim's name.

Such misuse can seriously harm a person's reputation and financial security. Victims may face embarrassment, social stigma, or loss of trust among friends and colleagues. Financial losses may also occur through unauthorized transactions or fraudulent schemes. Protecting personal information, using strong privacy settings, and being cautious while sharing data online are essential steps to reduce these risks.

4. Unauthorized Sharing of Private Content:

Unauthorized sharing of private content occurs when personal images or videos are distributed without the individual's permission. This act is a severe breach of privacy and trust, often carried out by acquaintances, former partners, or online attackers. Such content may be shared on social media, messaging platforms, or websites to embarrass, threaten, or control the victim. The consequences can be

deeply damaging, leading to humiliation, emotional distress, anxiety, and loss of self-confidence. Victims may also face social stigma and fear of public exposure. Strong legal protection, awareness, and secure digital practices are essential to prevent such violations.

5. Online Financial Crimes:

Online financial crimes are a growing threat, and many women become targets due to increasing use of digital banking, job portals, and online shopping platforms. Fraudsters often send fake job offers, create counterfeit shopping websites, or use phishing messages that appear to come from trusted institutions. These scams trick victims into sharing bank details, passwords, or one-time passwords, leading to unauthorized transactions and financial loss. In some cases, criminals also use social engineering techniques to gain trust before committing fraud. Awareness, careful verification of online offers, and the use of secure payment methods are essential to prevent such crimes.

Key Challenges in Ensuring Online Safety

1. Limited Cyber Awareness:

Many women lack knowledge about safe online practices such as privacy control settings, secure browsing, and scam detection.

2. Fear and Social Pressure:

Victims often avoid reporting cybercrimes because of social stigma, fear of public exposure, or lack of family support.

3. Ineffective Law Enforcement:

Although cyber laws exist, delayed investigations and limited technical expertise reduce their effectiveness.

4. Digital Divide:

Poor internet infrastructure and lack of access to cybersecurity tools, especially in rural areas, increase vulnerability.

5. Mental Health Impact:

Continuous exposure to online abuse can cause anxiety, depression, and loss of self-esteem.

Strategies to Protect Women from Cyber Threats

1. Promoting Digital Education

Training programs should focus on teaching women about online privacy, password management, identifying suspicious links, and reporting cybercrimes.

2. Strengthening Legal Protection

Governments should improve cyber legislation and establish fast-response systems such as cyber helpdesks and women-focused complaint cells.

3. Responsibilities of Technology Platforms

Social media companies must improve content monitoring, develop better reporting tools, and strengthen privacy settings.

4. Support Systems for Victims

Counseling services, legal assistance, and community support groups help victims recover emotionally and regain confidence.

5. Encouraging Safe Online Habits

Using two-factor authentication, antivirus software, secure networks, and regular software updates can significantly reduce cyber risks.

Role of Educational Institutions and Society

Educational institutions should introduce cybersecurity awareness programs and workshops. Students must be trained in responsible digital behavior and ethical online communication. Families and communities should encourage open discussions about online safety to build awareness and trust.

Statistical Evidence on Women and Cyber Threats

1. Global Prevalence of Online Abuse

- Studies show that **16% to 58% of women and girls worldwide** have experienced some form of online violence, including harassment, stalking, threats or digital abuse.
- In Arab States alone, **60% of women internet users reported online violence**; over **50% in Eastern Europe and Central Asia** have faced technology-facilitated abuse.
- A global UN Women-related press release states that **less than 40% of countries have laws protecting women from cyber harassment or stalking**, exposing gaps in legal safeguards globally.

2. Harassment and Violence Indicators

- Nearly **three in four (73%) women respondents** in international surveys have reported experiencing online violence such as abuse and harassment.
- In another global survey, **85% of women who use the internet have witnessed online violence**, and **38% reported they were direct targets of such violence**.
- Data from Plan International indicates that around **58% of girls have faced online harassment**, and **46% of women describe this harassment as sexist or misogynistic**.

3. Cyber Crime Trends in India

- Reports suggest cybercrime incidents against women registered on the **National Cybercrime Reporting Portal (NCRP)** in India have risen sharply — from about **22,188 cases in 2020 to 48,475 cases in 2024, a 118.4% increase**.
- According to Statista-linked research, **over 3,400 cases of cyber crime related to sexual harassment or exploitation** were reported in India in 2022.
- There are also regional cyberstalking impacts: in Maharashtra alone, **1,085 women were victims of cyberstalking or sexting between 2020 and 2025**, with scammers extorting over **₹51 crore** from them.
- National crime data indicate that overall cybercrimes against women rose in 2022 compared to 2021, contributing to broader increases in crimes against women.

Table 1: Cybercrime Cases Against Women in India

Year	Number of Cases
2020	22,188
2021	28,000 (Est.)
2022	35,000 (Est.)
2023	42,000 (Est.)
2024	48,475

The data show a clear and continuous rise in cybercrime cases against women in India between 2020 and 2024. Reported incidents increased from 22,188 in 2020 to 48,475 in 2024, with steady growth each year. This upward pattern indicates that online threats are becoming more frequent and widespread. The trend may be linked to increased use of smartphones, social media, digital payments, and online communication. While technology offers many benefits, it also exposes women to new risks. The growing number of cases highlights the urgent need for stronger cyber laws, better awareness, digital safety education, and improved technological protections.

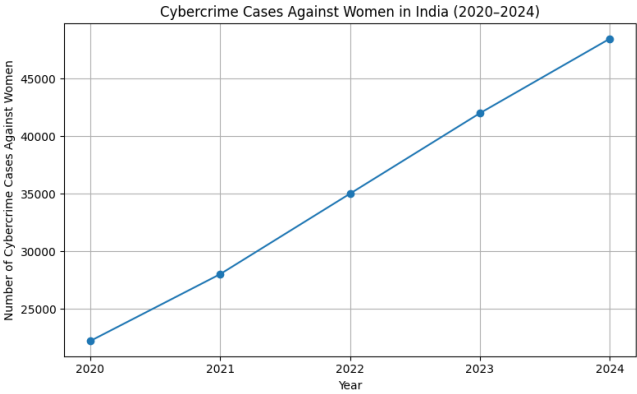
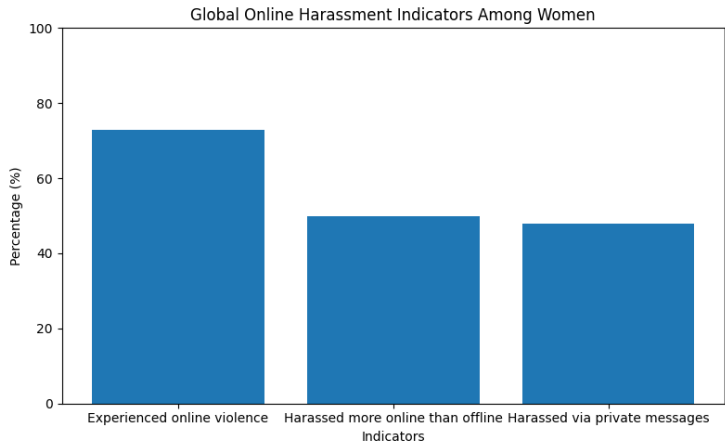


Table 2: Global Online Harassment Indicators

Indicator	Percentage
Experienced online violence	73%
Harassed more online than offline	50%
Harassed via private messages	48%



The table shows major indicators of online harassment faced by women worldwide. A large majority, about 73%, reported experiencing some form of online violence, indicating how common digital abuse has become. Around 50% stated that they faced more harassment online than in real life, suggesting that the internet can be a more hostile environment. In addition, 48% experienced abuse through private messages, showing that harassment often occurs in direct and personal forms. These figures highlight the

widespread nature of digital violence and underline the need for stronger safety measures, effective reporting systems, and greater awareness to protect women online.

Conclusion

The protection of women in the digital world requires a collective effort. While technology has improved access to information and opportunities, it has also introduced serious risks. Addressing these issues demands coordinated action from governments, educational institutions, technology companies, and society. By strengthening awareness, improving legal systems, and promoting responsible online behavior, a safer cyberspace for women can be created.

References

[1] Citron, D. K. *Hate Crimes in Cyberspace*. Cambridge, MA: Harvard University Press, 2014.

[2] Henry, N., & Powell, A. *Technology-facilitated sexual violence: A literature review*. Trauma, Violence, & Abuse, 19(2), 2018, pp. 195–208.

[3] Chisholm, N. *Cyberstalking and digital harassment: Patterns and impact*. Journal of Interpersonal Violence, 33(14), 2018, pp. 2226–2248.

[4] European Institute for Gender Equality (EIGE). *Cyber Violence Against Women and Girls*. Luxembourg: Publications Office of the European Union, 2021.

- [5] United Nations Broadband Commission. *Cyber Violence Against Women and Girls: A Worldwide Wake-Up Call*. UN Report, 2015
- [6] UN Women. *Online Violence Against Women and Girls: Global Report*. United Nations, 2021.
- [7] World Health Organization (WHO). *Violence Against Women Prevalence Estimates, 2018*. Geneva: WHO, 2021.
- [8] Alkahtani, M., Alomar, N., & Hernández-Ramos, J. *Women's awareness and practices toward cybersecurity risks: A systematic review*. *Journal of Information Security and Applications*, 53, 102558, 2020.
- [9] Kaur, H., & Sharma, N. *Online harassment and safety measures for women users in social media*. *International Journal of Computer Applications*, 175(18), 2021, pp. 20–26.
- [10] Kumar, R., & Gupta, S. *Cybersecurity awareness and gender: Challenges and solutions*. *International Journal of Cybersecurity*, 9(2), 2022, pp. 104–118.
- [11] National Crime Records Bureau (NCRB). *Crime in India Report*. Ministry of Home Affairs, Government of India, 2023.
- [12] Statista Research Department. *Cybercrime cases in India by type*. Statista Database, 2023.
- [13] Plan International. *Free to Be Online? Girls' and Young Women's Experiences of Online Harassment*. Global Report, 2020.