NEW ERA AGRICULTURE MAGAZINE

Cybersecurity for Women in India: Challenges, Initiatives & the Way Forward

Dr. Deepti Bhargava*, Dr. Saurabh*, Dr. Diksha Gautam* and Dr. Purvi Nishad*

Abstract: -

In an era marked by rapid digitization and increasing online participation, cyber security has become a critical concern, especially for women who are increasingly becoming targets of cybercrimes such as cyberstalking, online harassment, identity theft, and financial fraud. In India, where the government is actively promoting digital inclusion through initiatives like Digital India, ensuring the digital safety of women is paramount. This article provides an in-depth overview of the cybersecurity schemes, policies, and initiatives implemented by the Government of India and allied organizations to protect women in cyberspace.

Key words: digitization, cybercrime, cyber security, digital safety

Introduction

In the digital era, technology plays a crucial role in empowering women—offering them access to education, employment, and social networks. However, with increasing internet penetration, Indian women also face rising threats in cyberspace. From cyberstalking and online harassment to financial fraud and doxxing, digital crimes against women are on the rise, demanding urgent attention.

This article explores the landscape of **cybersecurity for women in India**, the **government initiatives** in place, and how women can protect themselves in the online world.

Cyber Threats Faced by Women

Women face a wide range of cybercrimes that often go underreported due to stigma, fear, or lack of awareness. Below are the major threats:

1. **Cyberstalking-** This involves persistent online harassment via emails, social media, or messages. Offenders may track location, monitor activity, or send threats to the women.
2. **Online Harassment and Trolling-** Online

Dr. Deepti Bhargava, Dr. Saurabh*, Dr. Diksha Gautam* and Dr. Purvi Nishad**

Assistant Professor,

Banda University of Agriculture, Banda, U.P.

Harassment and Trolling includes sending sexist, abusive, or threatening comments to women on social platforms. Women in public roles like journalists, activists, celebrities are frequent targets.

3. **Morphing & Deepfakes-** Photos of women are edited or manipulated to create fake nude images or videos and used for blackmail or defamation.
4. **Sextortion-** Criminals trick women into sharing private photos and later threaten to release them unless demands (often money or more photos) are met.
5. **Impersonation and Fake Profiles-** This includes **c**reating false profiles using someone's name/photos for scams or defamation. This often leads to social or professional damage.
6. **Revenge Porn-** Ex-partners share intimate content without consent, typically after a breakup.
7. **Phishing & Financial Frauds-** Targeted phishing messages trick women into revealing OTPs, passwords, or banking info. Scam jobs, fake shopping websites, and romance scams are common methods.
8. **Cyberbullying in Educational Settings-** Teen girls are often victims of bullying in school WhatsApp groups or on apps like Instagram and Snapchat.

Challenges and Gaps

- **Lack of Awareness:** Many women, especially in rural areas, are unaware of cybersecurity threats and how to report them.
- **Underreporting:** Fear of stigma and lack of trust in law enforcement contribute to low reporting of cybercrimes.
- **Limited Infrastructure:** Inadequate digital infrastructure and resources in rural areas hamper effective cybersecurity enforcement.
- **Gender Bias in Policing:** Gender insensitivity among police officers may lead to reluctance in registering or pursuing cases.

Legal and Government Support for Cybersecurity of Women

India has recognized the need for stronger cyber protection, especially for vulnerable groups like women and children. Here's how the government is addressing the issue:

1. **Cyber Crime Prevention against Women and Children (CCPWC) Scheme**

This scheme is launched by Ministry of Home Affairs (MHA) with the objective to strengthen cybercrime prevention and investigation capabilities, especially concerning crimes against women and children. Most important components of this

scheme are establishment of Cyber Crime Prevention Units, creation of a national cybercrime reporting portal (www.cybercrime.gov.in) and financial assistance to states/UTs to set up cyber forensic laboratories.

2. National Cyber Crime Reporting Portal

National Cyber Crime Reporting Portal is Specialized section for crimes against women and children. Official Website of this portal is https://cybercrime.gov.in. This portal is a platform which allows victims to report cybercrimes, especially against women and children, anonymously and securely. This portal is dedicated section for reporting crimes like cyber harassment, online stalking, and abuse and real-time tracking of complaint status. Platform allows women for filing of complaints (including anonymous reports for sexual content) and tracking status of complaints.

3. Indian Cyber Crime Coordination Centre (I4C)

This centre is launched by Ministry of Home Affairs. Major role of this centre is to act as a nodal point for coordination among various law enforcement agencies and stakeholders. This centre has two major functions. Firstly, it promotes research and innovation in cybersecurity and secondly, it provides training to law enforcement personnel to deal with cybercrimes against women.

4. Cyber Surakshit Bharat Initiative

This initiative is launched by Ministry of Electronics and Information Technology (MeitY). Its objective is to create awareness about cyber hygiene among citizens and government officials. This initiative focuses on sensitization and training, especially for women working in government or using public services.

5. Digital Shakti Campaign

This campaign is implemented by National Commission for Women (NCW), Cyber Peace Foundation, and Facebook aims empower women through digital literacy and cybersecurity awareness. Digital Shakti Campaign aims on digital literacy for girls and women. This creates awareness of cyber laws and reporting tools. Over 6 lakh women have been trained across India by training programs and workshops organised by this campaign.

6. SHE-Box

SHE-Box is **Sexual Harassment e-Box** for complaints of harassment at the workplace (including online abuse). This is managed by the Ministry of Women and Child Development. Official website of SHE-Box is https://shebox.nic.in

7. Cyber Crime Helpline

Toll-free helpline number to report financial frauds and urgent cyber threats is 55260.

Cyber Hygiene Tips

Every woman should practice cyber hygiene just like physical hygiene by using following considerations to avoid cyber frauds:

1. **Use Strong Passwords**

Every person should set strong password for in order to maintain their own security and set password combining uppercase, lowercase, numbers, and symbols. One should never reuse the same password across accounts.

2. **Enable Two-Factor Authentication (2FA)**

Use 2FA on important accounts like emails, bank apps, and social media.

3. **Set Social Media Privacy**

All women should make their profiles private and be careful with friend requests. Women should avoid sharing phone numbers or addresses online.

4. **Be Cautious with Links and Attachments**

Never click on suspicious links or download unknown files and check sender details before responding.

5. **Think Before You Share**

Avoid uploading personal content that can be misused and use watermarking apps on pictures if needed.

6. **Educate Yourself and Others**

Women should attend workshops, follow government advisories, and teach family members too.

Conclusion

Cybersecurity for women is a basic digital right. Cybersecurity for women in India is a critical component of ensuring safe and inclusive digital participation. Every woman deserves to feel safe online similarly as she should be in real life. While the government has taken commendable steps through schemes like CCPWC and initiatives such as Digital Shakti, continuous efforts are needed to bridge the digital gender divide and build a resilient ecosystem. With education, awareness, legal protection, and community support, women can navigate the digital world confidently and safely. Empowering women with knowledge, legal protection, and technological tools is key to their safety and confidence in the digital world.

References

1. Desai, J. (2025, February 5). Protecting women in the digital age: India's cybersecurity initiatives and their impact. *Medium*. Retrieved on 08/04/2025 from https://medium.com/@desaijay16sporty/protecting-women-in-the-digital-age-indias-cybersecurity-initiatives-and-their-impact-ba9b797bb041
2. Bairagi, T. (2023). Women and cyber crime in India: Factors and dynamics. *Academia.edu*. Retrieved on 10/04/2025 from https://www.academia.edu/124025244/Women_and_Cyber_Crime_in_India_Factors_and_Dynamics