

ISSUE 42 | NOVEMBER 2025

Every year from November 25 to December 10, the world observes the 16 Days of Activism Against Gender-Based Violence, a global campaign that measures our collective progress on one of the most entrenched human rights crises of our time. What began as a feminist initiative has evolved into a worldwide call to confront violence in all its forms.

This year's theme, "16 Days of Activism 2025: #NoExcuse for online abuse," brings the focus squarely onto the digital sphere. As deepfakes, cyberstalking and coordinated harassment become more widespread and sophisticated, the campaign emphasizes a simple truth: online harm is real harm. Safety must extend to digital spaces, and the internet cannot be allowed to operate without accountability.

Artificial intelligence is not only reshaping familiar patterns of gendered violence but also creating new ones. Researchers estimate that 90 to 95 percent of all online deepfakes are non-consensual pornographic images. The scale of the problem is rapidly increasing. The number of deepfake videos circulating online in 2023 was more than five times higher than in 2019, and deepfake pornography accounts for 98 percent of all deepfake content.

AI is also changing the landscape of impersonation and sextortion. New tools can generate interactive deepfakes that mimic human conversation, allowing bots to pose as real people and initiate contact with women and girls who have no idea they are speaking to an automated system.

AI is making
online abuse worse.

90—95%
OF DEEPFAKES ONLINE
SEXUALIZE WOMEN.

Practices like catfishing, once limited by effort and technical skill, can now be scaled with ease. This makes it far simpler to extract private information or lure victims into unsafe situations.

Doxing has become more sophisticated as well. Advanced language technology can scan women's posts for anything that might expose them to attack, including speaking out about harassment or challenging misogyny. Perpetrators can then use AI to craft highly personalized threats drawn from a victim's own words and data, heightening the emotional and psychological impact.

In the face of all this, it becomes imperative to raise awareness about how to protect ourselves and to intervene meaningfully if we are exposed to such risks. Several actions can help strengthen our safety online. The first is education. Building digital literacy, questioning the reliability of online sources, and understanding how AI-facilitated abuse works are essential foundations. Awareness of how these tools operate, and why they so often target women and girls, is a crucial starting point. Strengthening personal security matters as well. Using strong and unique passwords, turning on two-factor authentication, keeping profiles private, and regularly reviewing privacy settings can limit the information that can be collected or misused.

Collective action is equally important. Individuals can call on technology companies to take responsibility for the systems they build and profit from.

If you have been subjected to image-based abuse online, several resources can offer support and guidance. [StopNCII.org](https://stopncii.org) helps victims of revenge porn by preventing intimate images from being shared without consent. The site can generate a digital fingerprint, or hash, of an image, making it harder for others to distribute. [Take It Down](https://takeitdown.org) provides assistance in removing explicit content from the internet.

For emotional support, the [Cybersmile Foundation](https://cybersmilefoundation.org) offers a global service that helps those experiencing cyberbullying or online abuse and directs them to additional resources for protection and recovery.

Dr. Aastha Dang, a gender strategy specialist at Vertelo, Macquarie Asset Management, argues in her commentary “From Deepfakes to Deterrence: How Can India Build a Safer Digital World for Women” that protecting women online requires both legal and institutional reform. She calls for expanding gender-protection laws and workplace regulations to explicitly address technology-facilitated violations. For example, the POSH Act could be updated to cover online harassment, misuse of personal data, and the preventive responsibilities of employers, including awareness programs, safe digital practices, and protective tools.

Organizations, she notes, also need robust systems for gender-disaggregated data to identify bias and strengthen accountability for AI-enabled harms. Regulators should require regular risk assessments, harm-reduction measures, and transparent incident reporting from both platforms and employers. Finally, explicitly criminalizing offenses such as deepfake abuse, identity theft, and targeted digital harassment within anti-violence laws could create stronger deterrents. These reforms, Dang suggests, should ensure that anonymity protects vulnerable users rather than shielding perpetrators.

The rise of AI-driven abuse makes it clear that the fight against gender-based violence must evolve alongside technology. Awareness, personal digital safety, collective action, and legal reform are all critical pieces of a comprehensive response. By educating ourselves, securing our online presence, supporting survivors, and holding platforms and institutions accountable, society can begin to ensure that the digital world is as safe and just as the physical one should be. The 16 Days of Activism in 2025 is a reminder that there is no excuse for online abuse and that meaningful change requires both vigilance and action.

WHAT CAN YOU DO IF YOU SPOT ONLINE ABUSE? 🙄

Save the evidence.

Block and report it.

Secure your accounts.

Tell someone you trust.

The monthly newsletter from the Committee for Managing Gender Issues (CMGI) is an attempt to initiate conversations on sexual harassment. We would love to have the community participate. Please reach out to Geetika Sharma at geetikas@iima.ac.in for queries, submissions, and/or feedback.

If you feel you have been subjected to sexual harassment or if you would like to make any suggestions regarding curbing sexual harassment on campus, please reach out to us at: Email: chr-cmgi@iima.ac.in. Please note that any communication with the CMGI is strictly confidential.