Protecting women and children in cyberspace

by Md Motiar Rahman 01 February, 2025, 00:00

The police introduced an all-women unit to fight growing online abuse and harassment of women. | The Swaddle

THE digital revolution has transformed societies worldwide, creating opportunities for communications, education and economic growth. However, as the virtual world expands, it also brings challenges, particularly in ensuring the safety of vulnerable groups such as women and children. In Bangladesh, the rapid adoption of technology has exposed such groups to unprecedented risks such as online harassment, cyber-bullying, exploitation and data breaches. Despite efforts to address these issues, existing technological and legal mechanisms remain insufficient to guarantee a safe online environment. It is imperative to explore the challenges faced in creating safe cyberspaces for women and children, focusing on the gaps in technological and legal frameworks and offering recommendations for improvement.

Rise of cyber threats

THE internet is a double-edged sword for women and children in Bangladesh. While it offers access to education, social interaction and professional opportunities, it also exposes them to significant risks.

Women are disproportionately subjected to cyber harassment, which often takes the form of abusive messages, threats and unwanted sexual advances on social media platforms, messaging apps and online forums. Perpetrators exploit the anonymity offered by the internet to intimidate and humiliate their targets. This harassment can range from persistent stalking and offensive comments to more severe acts such as doxxing, where a victim’s personal information is shared publicly without consent. Women who speak out on social or political issues are particularly vulnerable as they often face coordinated campaigns of online abuse aimed at silencing their voices. The psychological toll of such harassment can lead to anxiety,

depression and even withdrawal from online spaces, curtailing women's freedom of expression and participation in digital communities.

Cyber-bullying has become a major threat to children, with social media platforms, messaging apps and online gaming environments serving as primary hotspots. Perpetrators use these spaces to spread rumours, share humiliating content and send threatening or abusive messages. Unlike traditional bullying, cyber-bullying invades the safety of children's homes. Victims often face social isolation, academic struggles and severe emotional distress, which can sometimes lead to self-harm or suicidal thoughts. Strangers pretending to be peers on gaming platforms or chatrooms, manipulating children into compromising situations or subjecting them to verbal abuse during interactions, further heighten the risks.

The internet has become a fertile ground for criminals engaging in online exploitation, targeting both women and children. Children are often lured into sharing explicit images or videos through grooming tactics, with the material being used for child pornography or trafficking purposes. Women, on the other hand, are frequently blackmailed through non-consensual image sharing, where perpetrators threaten to leak private photos or videos unless demands, often financial or sexual, are met. Revenge porn, where intimate images are shared online by former partners without consent, is another form of exploitation that disproportionately affects women. The consequences are devastating, including reputational damage, the loss of employment and severe psychological trauma. Victims are often left with limited legal recourse due to the complexities of tracking down and prosecuting offenders, particularly when crimes involve international elements.

Phishing schemes and online fraud increasingly target women and children, exploiting their lack of awareness about cyber-security threats. Phishers often disguise themselves as legitimate entities such as banks or government agencies and trick victims into sharing sensitive information such as passwords, credit card details or personal identification numbers. Children are particularly susceptible when playing games or entering contests, unknowingly exposing family financial data. Women are frequently targeted with scams promising lucrative job opportunities, scholarships or romantic relationships only to be defrauded of money or personal information. Once compromised, victims may face financial losses, identity theft or even blackmail, with fraudsters using the stolen data to exploit them further. This disrupts lives and undermines trust in online platforms and services.

In Bangladesh, the problem is exacerbated by the lack of awareness of digital safety and the limited availability of robust preventive tools. Social taboos and victim-blaming further discourage women and children from reporting cyber incidents.

Technological challenges

DESPITE remarkable technological advancements, creating and maintaining safe cyberspaces for women and children remain a complex and pressing issue. Several technological challenges continue to hinder efforts toward ensuring a secure online environment.

Inadequate privacy and security: Many digital platforms, including social media, messaging apps and online forums, lack robust privacy and security settings. This makes it relatively easy for predators, stalkers and other malicious actors to target users. While some platforms provide basic tools for privacy, they often require users to navigate complex settings, which can be overwhelming for individuals with limited digital literacy. Additionally, platforms often fail to act swiftly or adequately when abuse or harassment is reported. Victims may face delayed responses or outright neglect, leaving them vulnerable to continued harm. Furthermore, loopholes in security protocols such as weak encryption or insufficient safeguards against account hacking exacerbate the risks faced by women and children online.

Weak content moderation: Content moderation remains one of the most significant technological challenges in ensuring online safety. Algorithms designed to identify and remove harmful content frequently under-perform when applied to non-English languages, including Bangla. As a result, abusive messages, explicit imagery and other harmful content targeting Bangladeshi users often go unnoticed and unaddressed. This gap in moderation allows harmful content to proliferate unchecked, creating a hostile and unsafe environment for women and children. Additionally, the reliance on automated moderation systems, without adequate human oversight, often results in either over-censorship or under-enforcement, failing to strike the right balance in protecting users.

Limited digital literacy: A significant portion of the population, particularly women and children, lacks the digital literacy needed to navigate cyberspace safely. Many users are unaware of basic cybersecurity practices such as creating strong passwords, recognising phishing attempts or avoiding suspicious links. This lack of awareness leaves them particularly vulnerable to online threats, including scams, identity theft and exploitation. Children, in particular, may unknowingly share personal information or engage with strangers online, increasing their susceptibility to cyber-bullying or grooming. Women, on the other hand, are often targeted with sophisticated scams, exploiting their limited technical knowledge to compromise their privacy or financial security.

Absence of localised tools: The scarcity of technological tools and solutions tailored to the

Bangladeshi context further exacerbates the problem. Most cybersecurity tools, reporting mechanisms and helplines are designed for a global audience, often overlooking the specific needs of Bangladeshi users. For instance, a few cybersecurity tools or reporting platforms are available in Bangla, limiting accessibility for non-English-speaking users. Similarly, women and children often struggle to access localised resources such as helplines or apps that provide targeted support for issues like online harassment, exploitation or fraud. The lack of culturally and linguistically appropriate tools leaves many users without effective means to address or mitigate online risks, widening the digital safety gap.

Legal framework and shortcomings

THE draft Cyber Protection Ordinance 2024 introduces measures aimed at improving the safety of women and children in cyberspace, including criminalising ‘revenge porn’ to address the non-consensual sharing of intimate content. While these updates reflect progress in protecting vulnerable groups, the ordinance has removed certain provisions, such as those addressing cyberbullying and has dropped nine controversial sections, including warrantless search. The law enforcement’s authority to conduct search, seizure and arrest is now limited to cyber-attacks targeting critical information infrastructure. Despite the adjustment, the ordinance continues to face criticism for its potential misuse as cyber security experts warn that it retains repressive elements from the previous Cyber Security Act 2023 to ensure the ordinance upholds fundamental rights.

Critics and other stakeholders argue that the ordinance fails to address key concerns of marginalised groups such as national communities, women with disabilities and rural populations. These groups remain vulnerable to cyber harassment, AI-enabled impersonation and other digital crimes, with no clear legal mechanisms to seek justice or support. The ordinance’s punitive nature, the centralisation of power with law enforcement and the lack of procedural safeguards raise concern about privacy and the freedom of expression. Stakeholders advocate for incorporating international best practices, a clearer protection for marginalised groups and broader public consultations to balance safety and individual rights effectively.

Cultural and social barriers

IN BANGLADESH, deeply-rooted cultural norms and societal attitudes pose significant

challenges to creating safe cyberspaces for women and children. Victim blaming and stigma often deter victims of online harassment or exploitation from seeking justice as they face unjust scrutiny over their behaviour, attire or online activity. Women, in particular, fear being labelled as ‘immodest’ or ‘reckless’, which silences many even in severe cases of abuse. Patriarchal attitudes and traditional gender roles further exacerbate the issue by discouraging women and children from fully engaging in digital spaces, shifting the focus away from holding perpetrators accountable and instead imposing restrictions on victims’ freedoms. This environment perpetuates a culture of impunity and limits the ability of women and children to confidently navigate cyberspace.

The lack of digital awareness among parents and educators worsens these challenges as many guardians lack the knowledge to guide children on safe online practices or recognise emerging cyber threats like cyber-bullying and grooming. Cultural taboos surrounding cyber issues also hinder open discussions about online harassment or exploitation, leaving victims without support and enabling crimes to go unreported. Additionally, societal reluctance to embrace digital change creates a generational gap in understanding cyberspace, leaving young people vulnerable and older generations ill-equipped to address evolving digital risks. These barriers collectively undermine efforts to build a safe and empowering digital environment for all.

Safe cyberspace

CREATING a safe cyberspace requires a comprehensive, multi-faceted approach that integrates technological interventions, legal reforms and awareness initiatives. Technological efforts should prioritise developing localised tools with Bangla-language support, enhanced privacy settings and stronger content moderation for non-English content. Mandatory age verification processes, robust content moderation policies and local accountability mechanisms for tech companies are also essential. Legal reforms must address gaps in the ordinance by clearly defining offences such as cyber-stalking, online grooming and identity theft while introducing a provision to safeguard personal information. Establishing specialised cybercrime units, gender-sensitive fast-track courts and strict regulations for social media platforms can provide a solid framework for tackling online harassment, exploitation, and abuse.

Preventive measures such as digital literacy campaigns, integrating cyber safety into school curriculums and targeted awareness programmes of law enforcement are equally critical. Nationwide campaigns can educate the public about cyber threats and reporting mechanisms,

while schools, community organisations and media outlets can promote safe online practices. Additionally, robust support systems for victims such as cybercrime hotlines, dedicated police help desks and access to psychological and legal assistance should be prioritised. To combat cross-border cyber-crimes, Bangladesh must align its national laws with global standards by adopting international conventions such as the Budapest Convention on Cybercrime and fostering international cooperation. Public-private partnerships can further enhance technological resources and accountability, ensuring a safe, inclusive cyberspace for women and children while reducing vulnerabilities and building public trust.

The safety of women and children in cyberspace is an urgent issue that demands immediate attention. While technology offers immense opportunities, it also exposes vulnerabilities that must be addressed through robust technological solutions, comprehensive legal frameworks and widespread awareness. For Bangladesh, ensuring safe cyberspaces is not just a matter of individual security but a cornerstone of equitable digital transformation. By addressing the challenges, Bangladesh can create a safe, inclusive digital environment where women and children can thrive without fear.

Dr Md Motiar Rahman is a retired deputy inspector general.

Tags #women #Children #cyberspace

Read More

Early action must against wilful loan defaulters

Feb 01, 2025

Recent News

Protecting women and children in cyberspace

Early action must against wilful loan defaulters

Govt should redouble efforts to dispel economic disparities

Samsung Electronics posts 129.85pc operating profit

Hajj Finance holds 117th board meet

NEWAGE

Editor: Nurul Kabir, Published by the Chairman, Editorial Board ASM Shahidullah Khan on behalf of Media New Age Ltd.

Hamid Plaza (4th floor), 300/5/A/1, Bir Uttam CR Datta Road, Hatirpool, Dhaka-1205
PABX: +8802 41062247-50, Fax: +8802-41062245

newage.editorial@gmail.com

For Advertisement, Cell: +8801849 263831
Email: adnewage@gmail.com

ABOUT

CONTACT

ARCHIVE

DISCLAIMER & PRIVACY POLICY

ADVERTISEMENT

TERMS & CONDITIONS

SITEMAP