

FOR WIDE DISSEMINATION

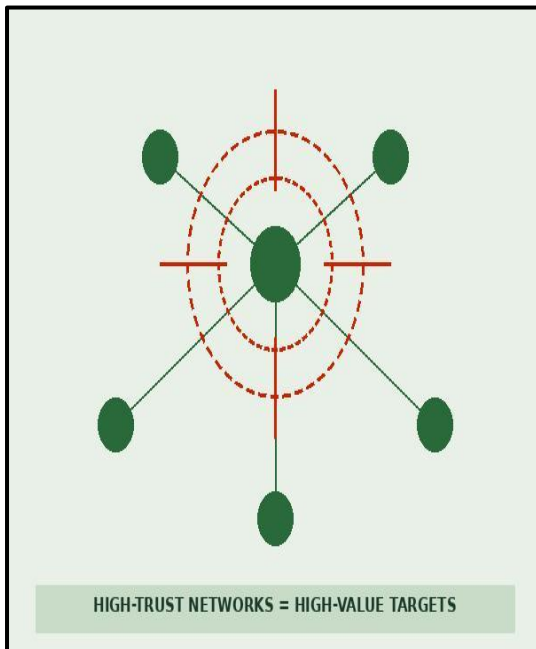
Advisory for Women

Detecting and Countering False Information in Your Digital Environment

A Message to the Women of India

The information ecosystem of India is constantly under attack from an adversarial stance. Women, who form the main links of information networks within families, as well as the key receivers of health and community-related information, are systematically attacked through information warfare. This alert comes out of a recognition of your intelligence, social significance and influence to become the most potent agents of information truthfulness. The ten steps below that are illustrated are realistic, actionable and immediately implementable.

Ten-Point Advisory

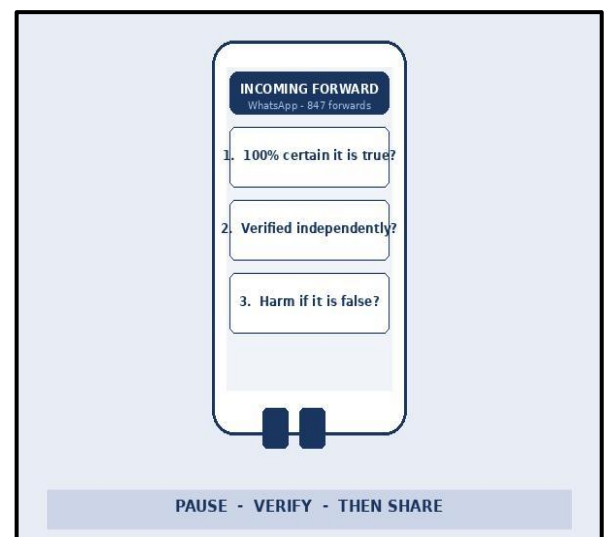


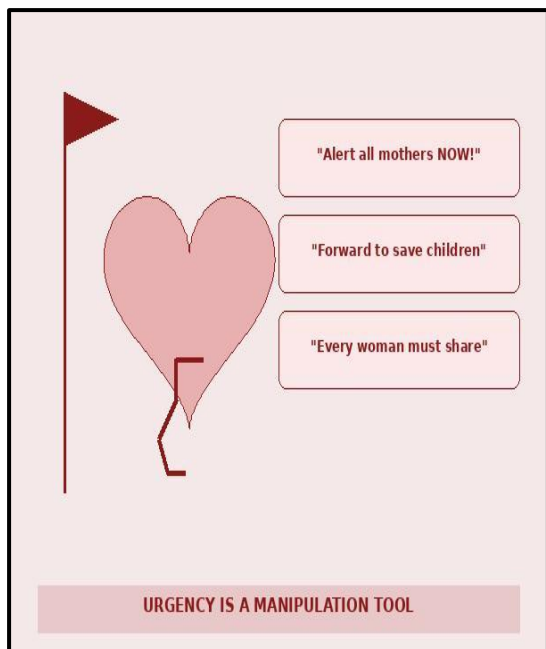
1. **Recognise That Women Are Priority Targets for Information Operations.**

The literature on computational propaganda has shown that there is evidence that women, especially women who manage family WhatsApp groups or women in high-trust community networks, are more likely targets of fake news campaigns. This is because women have both high-trust and high-reach networks. The people conducting the adversarial information campaigns strategically craft content for sharing within these networks. The first step in being resistant to such attacks is to realise that you are a target.

2. **Apply the Before-I-Share Standard Before Every Forward.**

Set your own criteria before you forward anything through WhatsApp, Facebook or Telegram. The three criteria are - Do I have 100 percent confidence about its veracity? Have I independently confirmed this from sources other than those which circulated this message? What would be the most severe repercussions of it being false? Unless you can satisfy all three criteria, refrain from sharing.



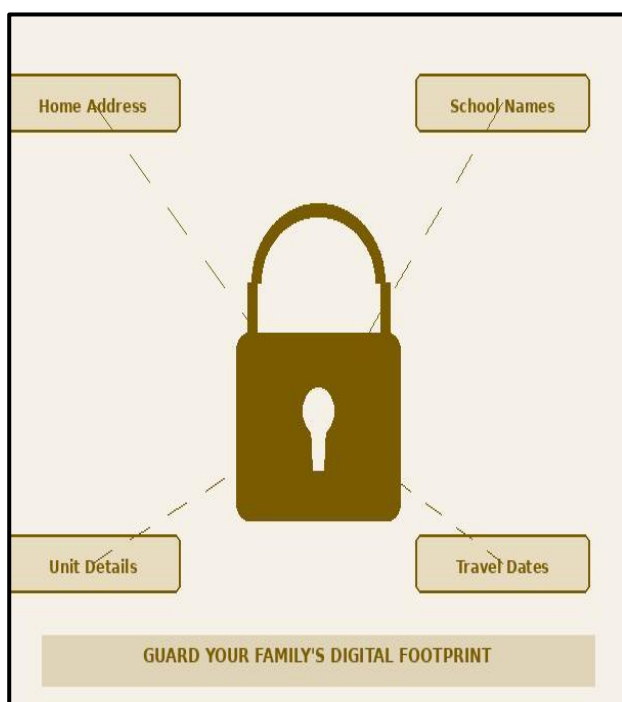
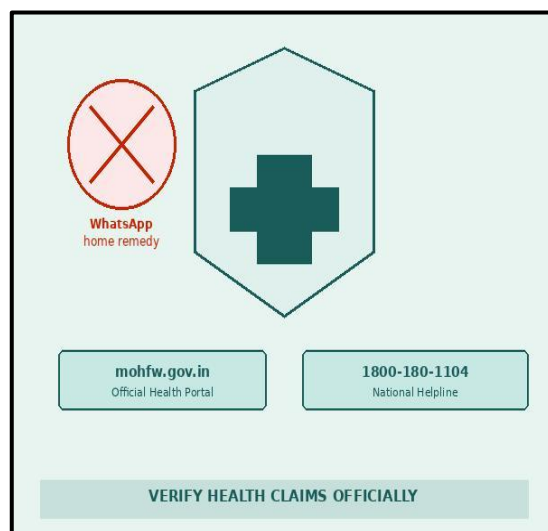


3. Identify Emotional Manipulation in Message Design.

Misinformation that targets women usually uses emotions that include the safety of one's children, safety within families, religion and honour of the community. The messages that start with statements like 'Alert all moms...' 'All Indian ladies should forward this message...' and 'Forward for the safety of your children...' are designed in such a way to circumvent logical reasoning and activate protective emotions. An increased level of emotional urgency in any message is simply a form of manipulation; watch out for it.

4. Verify Health and Medical Information Rigorously.

Health information becomes viral very quickly in groups of women since the significant influence of women within the family on making decisions regarding healthcare cannot be ruled out. Viral warnings concerning health could result in physical damage, either because such messages advise people to take part in activities that might put them in danger or spread information about epidemics which has not been verified yet. Prior to taking any action based on the health information shared, make sure to do so.

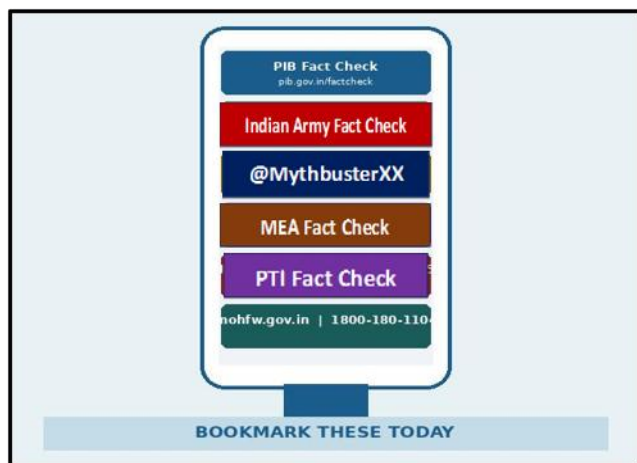


5. Protect Your Digital Identity and Personal Data.

Adversaries conducting hostile information warfare use social media profiles of women to gather their personal information, including photographs, mobile phone numbers, residential addresses, the name of their children and even the spouse. These personal pieces of information can be used for generating morphed pictures to blackmail or tarnish the reputation of the individuals. Update privacy settings on all social media every three months. Do not share your children's schooling information, photographs in uniform, your residential address, location name or travel plans.

6. Become the Fact-Checking Authority in Your Family Network.

In most Indian WhatsApp groups of families, women hold a position of social authority implicitly. You should use this position to create a culture of verification. Once you have identified and fixed a mistake in the message, you should pass on the correction with a link to a source, politely, without embarrassing the sender of the message. You should remember that you want to create a culture of verification and not make people feel bad for having been tricked.

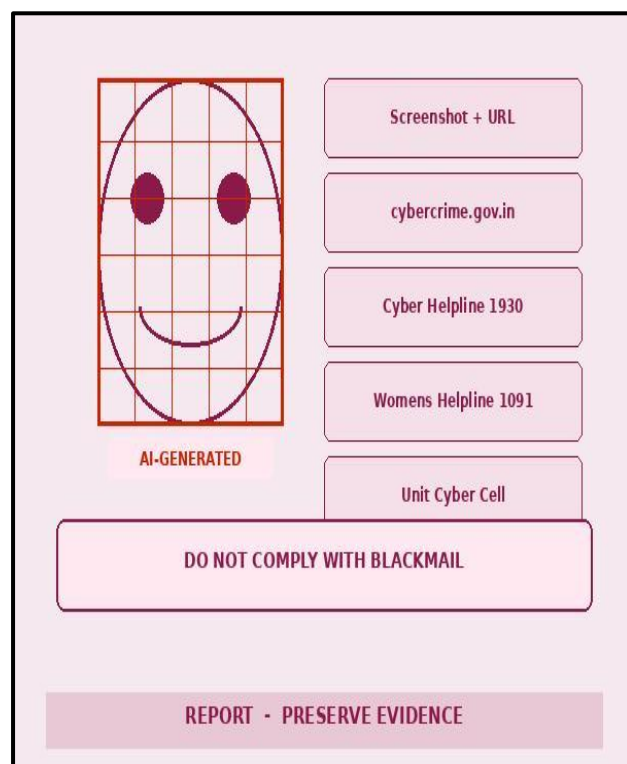


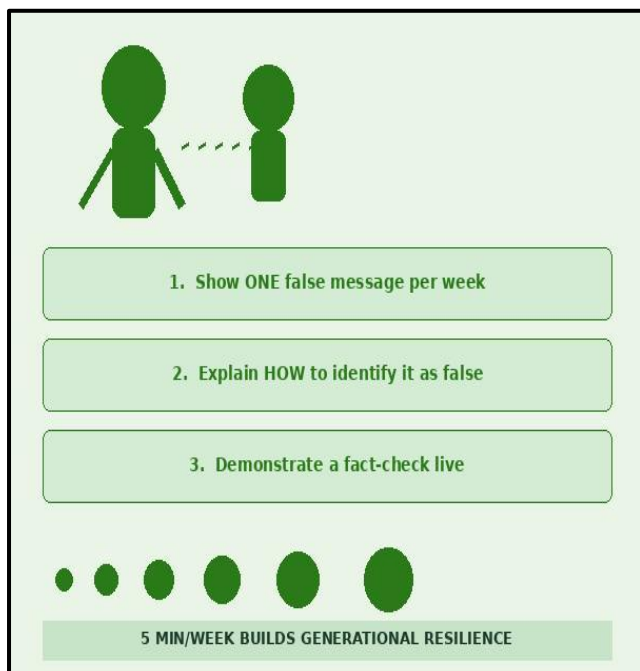
7. Bookmark Official Fact-Checking Resources Today.

Save these authenticated websites to your phone right away: PIB Fact Check website (pib.gov.in/factcheck), MEA Fact Check (@MEAFactCheck) on X and Indian Army Fact Check (@indianarmyfactcheck on Instagram and @MythbusterXX on Twitter).

8. Recognise Deepfake and Morphed Image Attacks.

Morphed images created using the AI technology of merging your face on to another body image are being employed as weapons of harassment, blackmail and reputation ruination against the families of the Armed Forces. In case either you yourself or your loved one fall prey to such an assault, then the following steps should be taken immediately. Refrain from meeting the blackmailer's demands. Save all related data including the web address, account name and timestamp. Register complaints with cybercrime.gov.in or call 1930 for the Cyber Helpline. Contact Women's Helpline at 1091.





9. Teach Children in Your Family the Same Skills.

Children witnessing adults verifying information before dissemination acquire information hygiene as a part of their nature. Spend five minutes every week; present a fake news article to the kids in your household, teach them how to spot the falsehood and guide them through the process of verifying information using an information-checking website. You have thus ensured that your family remains resilient to information warfare for generations to come.

10. Report, Record and Refuse to Be Silenced.

If you come across any fake or fabricated data, file a complaint immediately. Utilise the report mechanisms provided by the social media site itself. If the information pertains to the military and/or represents a matter of national security, file a complaint with cyber cell as also raise it via a DM on Indian Army Fact Check accounts on X / Instagram / Facebook / Youtube / Telegram. Take screenshots of your complaints for possible future use in evidence. Participation in ensuring information integrity in India is your duty as a citizen.

