

FOOD FOR THOUGHT

BETTER SAFE THAN SORRY

Avoid sharing personal pictures, videos or anything which can potentially become a reason for embarrassment later.

Perpetrators mostly disguise under Social Networking platforms using fake profiles. If someone seems suspicious, block them. If someone approaches wrongly, report them.

NIP IT IN THE BUD

FOLLOW @CYBERDOST

Follow @CyberDost on Twitter for Cyber Safety & Cyber Security awareness by Ministry of Home Affairs, Govt. of India.

TO REGISTER A COMPLAINT

ONLINE

National Cyber Crime Reporting Portal: Report Anonymously or Report & Track
<https://www.cybercrime.gov.in>

National Commission for Women (NCW) – Complaints Registration and Monitoring System
<http://ncwapps.nic.in/onlinecomplaintsv2/frmlInstructions.aspx>

Register complaints through email at: ncw@nic.in

OFFLINE

File written complaint at your jurisdictional police station or Cyber Crime Police Station (if present in the city)

For any emergency, contact National Women Helpline Number: **181**

#StayCyberSafe



ONLINE SAFETY FOR WOMEN

A simple guide covering Cybercrimes against Women, safety tips & grievance redressal mechanisms for Digital Safety & Well-being.



#StayCyberSafe

<https://www.dsci.in/content/stay-cyber-safe>



dsci.connect



DSCI_Connect



data-security-council-of-India



dscivideo

TYPES OF CYBERCRIME AGAINST WOMEN

Get acquainted with the common terms which are your Right to Fight

● **Cyber Harassment**

An act which includes any form of use of the internet to harass, threaten or embarrass in the form of emotional, sexual or social abuse.

● **Cyber Stalking**

An act where an individual uses the cyberspace to follow, bother or frequent someone continuously to the extent of causing distress; the motive being obsession, retribution, sexual harassment, etc.

● **Cyber Bullying**

An act where someone through electronic means intentionally and aggressively uses hurtful words, derogatory comments, fake information, sensitive material concerning someone to cause embarrassment/distress repeatedly and overtime.

● **Morphing**

An act where the perpetrator edits and uploads an original picture with something else (most cases with obscene images) and misuses it to defame, blackmail or as an act of revenge against someone.

● **Cyber Defamation**

An act when someone intentionally tries to infringe 'another person's right to his good name'. It involves publishing defamatory material against any person through electronic mediums.

● **Cyber Extortion**

An act of gaining or tracking someone's information without their knowledge and then circulating or threatening to circulate, sensitive content, private images or videos with a motive of personal vendetta or monetary gains.

CYBER SECURITY BASICS

for a safer Internet experience

- Create strong passwords with alphanumeric characters and never share them.
- Secure your systems with antivirus, anti-spyware, and upgrade to the latest OS.
- Don't give unnecessary camera/microphone permissions to apps. Be mindful of the purpose before you allow.
- Never leave your laptop open at public places, café or workstations. Lock them immediately.
- Don't install applications shared over email/chat by anyone. Malicious codes can turn on webcam, record audio without knowledge. Always download from trusted sources.
- Be watchful of phishing scams offering huge discounts on shopping, jewellery, or freebies.

ONLINE SAFETY PRACTICES

for Social Networking Platforms

- Don't share personal information with unknown persons or someone who shows interest in you.
- Don't meet online acquaintances alone for the first time. Prefer cafes, public places.
- Never feel weird turning down requests; be it a friend request or a proposal. You aren't liable to give reasons for your choices.
- Do not post content revealing too much personal information such as location, address, contact number, etc.
- Don't fill forms online through email/chat asking for biodata in the name of matrimony.
- Customize your default privacy settings for aspects like who can view profiles, posts, add in groups, tag, chat, identity, etc.

MOST SOCIAL PLATFORMS HAVE A CLEAR PROCEDURE IN PLACE FOR SETTING USER PRIVACY AND REPORTING ABUSE TO PROTECT USERS FROM ONLINE ABUSE AND CYBERCRIMES.

