Cyber Crime and Youth (Threats, Impact and Precautions)

What we will be discussing…

- What is Cyber Crime
- Common Types of Social Media Crimes
- Steps taken by Government for ensuring Cyber Safety – Reporting and Awareness (NCRP, 1930, CCPWC, Cyber dost etc)
- Cyber safety (Dos and Donts)
- Prevalent Financial Frauds

What is Cyber Crime?

Unlawful or criminal act when a computer or computer resource is:

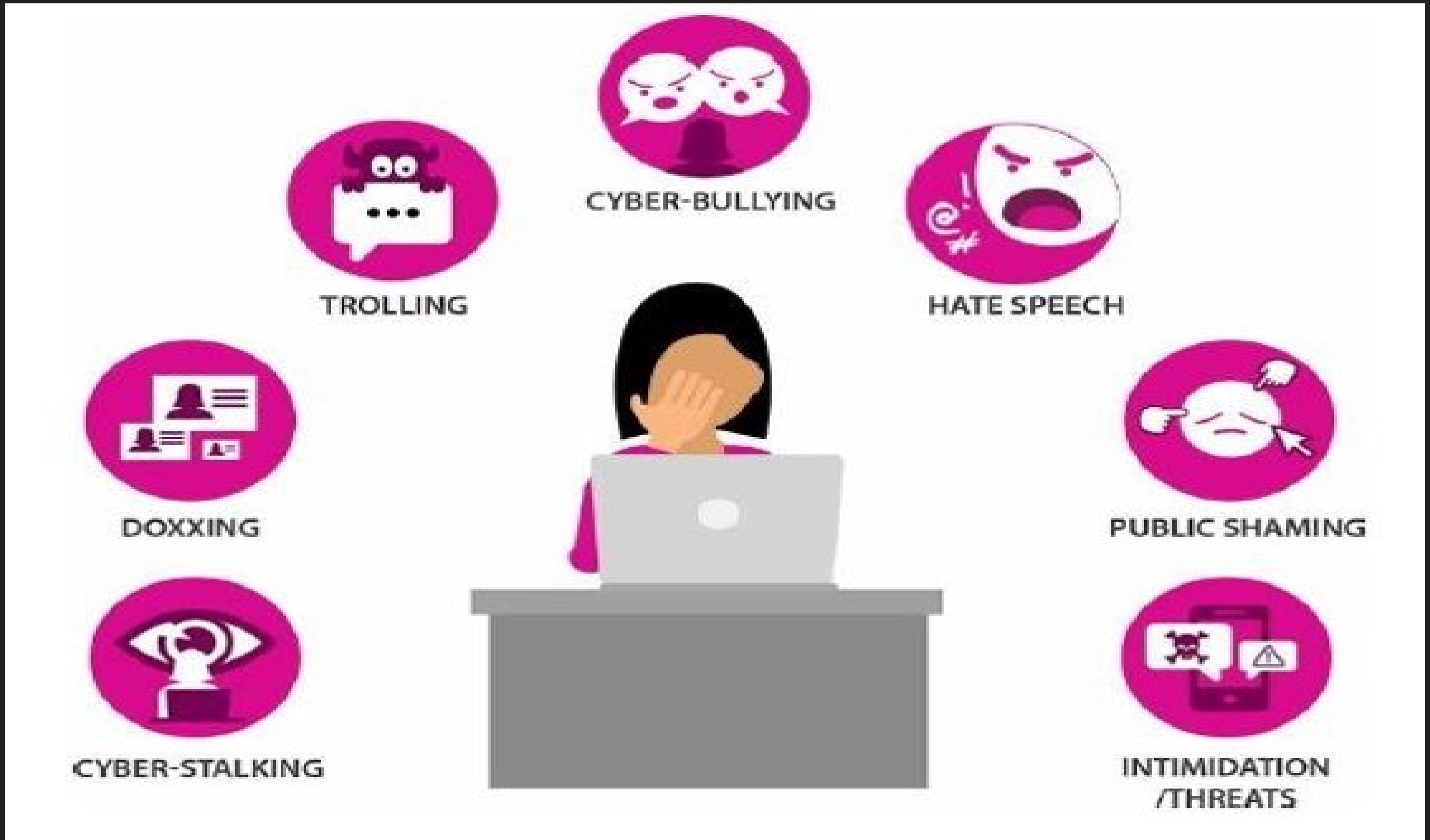
- A target of criminal act

- A tool to commit the crime

OR

- Is incidental to the commission of crime.

Common types of cyber crimes



Cyber Bullying

Act of:

- Sending, posting, sharing negative, harmful and demeaning content regarding others.
- Sharing personal or private information which could cause embarrassment or humiliation to others.

Cyber Stalking

- Posting harassing or threatening messages on someone’s social media profile/ blogs
- Posting personal advertisements in victim's name
- Hate speech, i.e. the language that denigrates (criticizes unfairly), insults, threatens/targets an individual based on their identity and other traits
- Accessing someone’s e-mail or social media accounts

CYBERSTALKERS
Are Not
Ugly, Stupid or Easily Spotted
In Fact, Most Were Your
Lovers, Friends, Business
Associates and Family Members
www.ipredator.co

Identity Theft

Act of using someone else's Personal Identity Information without their permission such as:

- their name
- identification
- credit card number etc.

Doxxing

Act of revealing identifying information about someone online, such as:

- Their real name
- Home address
- Workplace
- Phone
- Financial
- Or any other personal information.

Sextortion

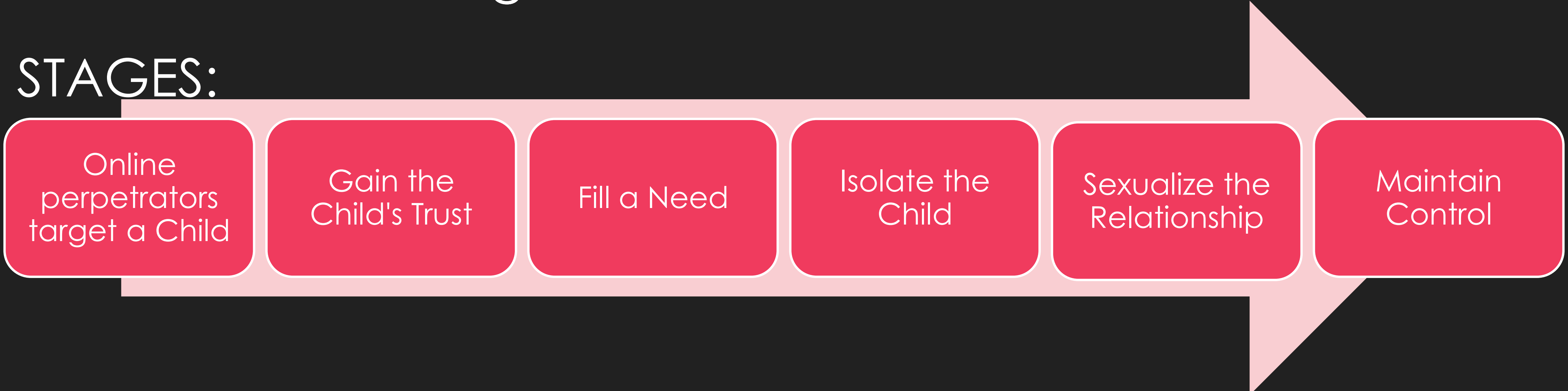
Threatening to distribute private and sensitive material using an electronic medium if he/ she doesn't provide images of a sexual nature, sexual favors, or monetary benefits

File photo: ST

Cyber Grooming

When a person builds an online relationship with a minor/young person and tricks or pressures him/her into doing sexual act.

STAGES:



Revenge Pornography

Act of circulating private and sexually explicit images and videos of sexual acts online without the consent of the individual.

- Mostly partners/friends/ acquaintances

Job fraud

Online Job Fraud is an attempt to defraud people who are in need of employment by giving them false hope/ promise of better employment with higher wages.

Phishing

Phishing involves stealing personal information such as:

- Customer ID,
- IPIN,
- Credit/Debit Card number, Card expiry date, CVV number, etc.
- Done through emails/SMSs that appear to be from a legitimate source.

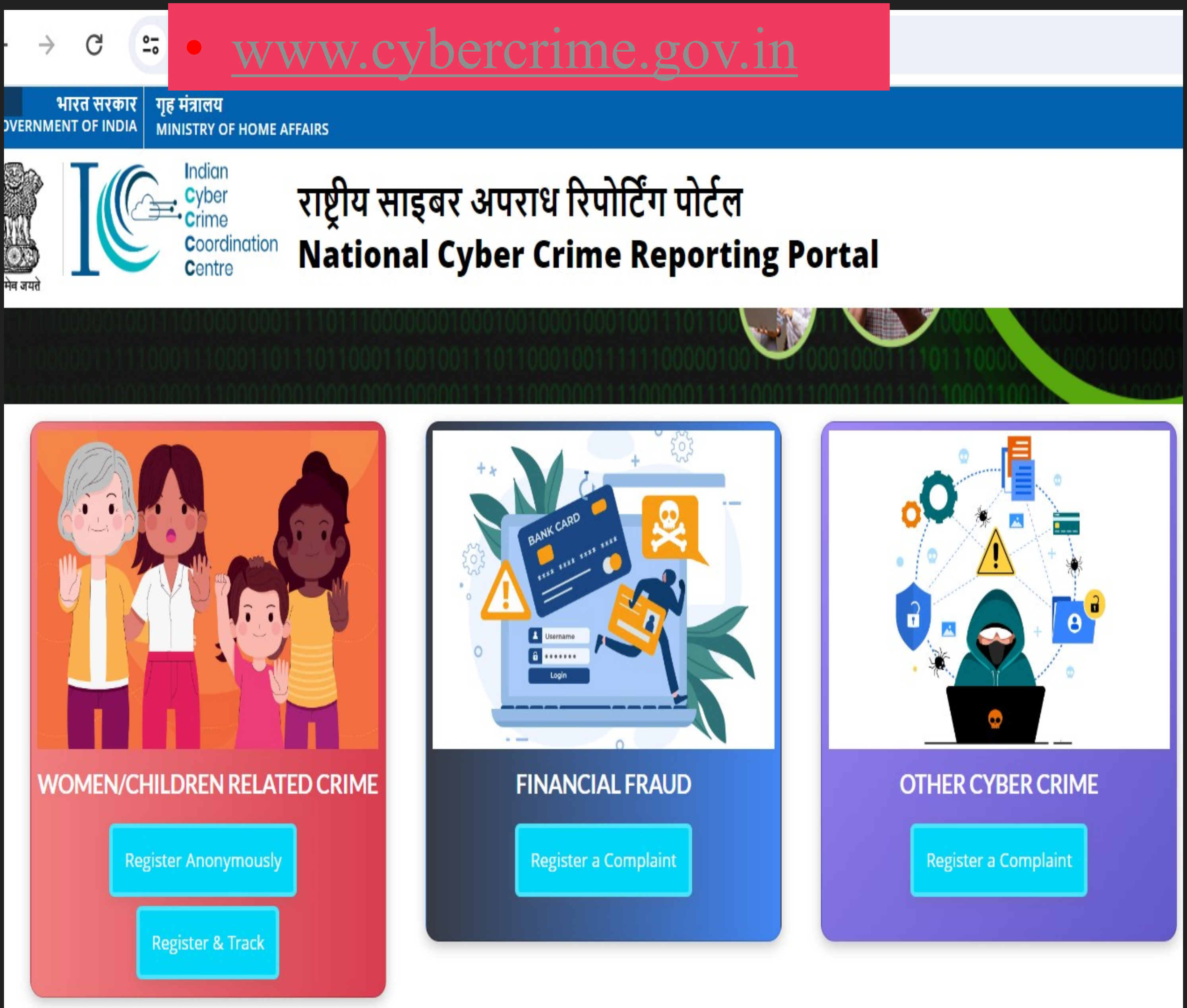
Vishing

Vishing is an attempt where fraudsters try to seek personal information through a phone call or VOIP call.

Steps taken by the Government for ensuring Cyber Safety

National Cyber Crime Reporting Portal

- to enable public to report incidents pertaining to all types of cyber crimes,
- with a special focus on cyber-crimes against women and children
- 1930 helpline (financial fraud)



- www.cybercrime.gov.in

भारत सरकार
OVERNMENT OF INDIA

गृह मंत्रालय
MINISTRY OF HOME AFFAIRS

Indian
Cyber
Crime
Coordination
Centre

राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल

National Cyber Crime Reporting Portal

Cyber Financial Fraud Helpline - 1930

Victim calls 1930 helpline to report Financial Fraud

LEAs raise complaint on behalf of Victim on the Portal.

Timely reported Financial fraud money will be put on hold by the Nodal Officer

Cyber Crime Prevention against Women and Children (CCPWC) Unit

deals with only these 4 Categories-

1. Child Pornography/Child Sexual Abuse Material (CP/CSAM)
2. Rape/Gang Rape-Threats
3. Publishing or transmitting of material containing Sexually Explicit act in electronic form.
4. Publishing or transmitting Sexual Obscene Material in electronic form.

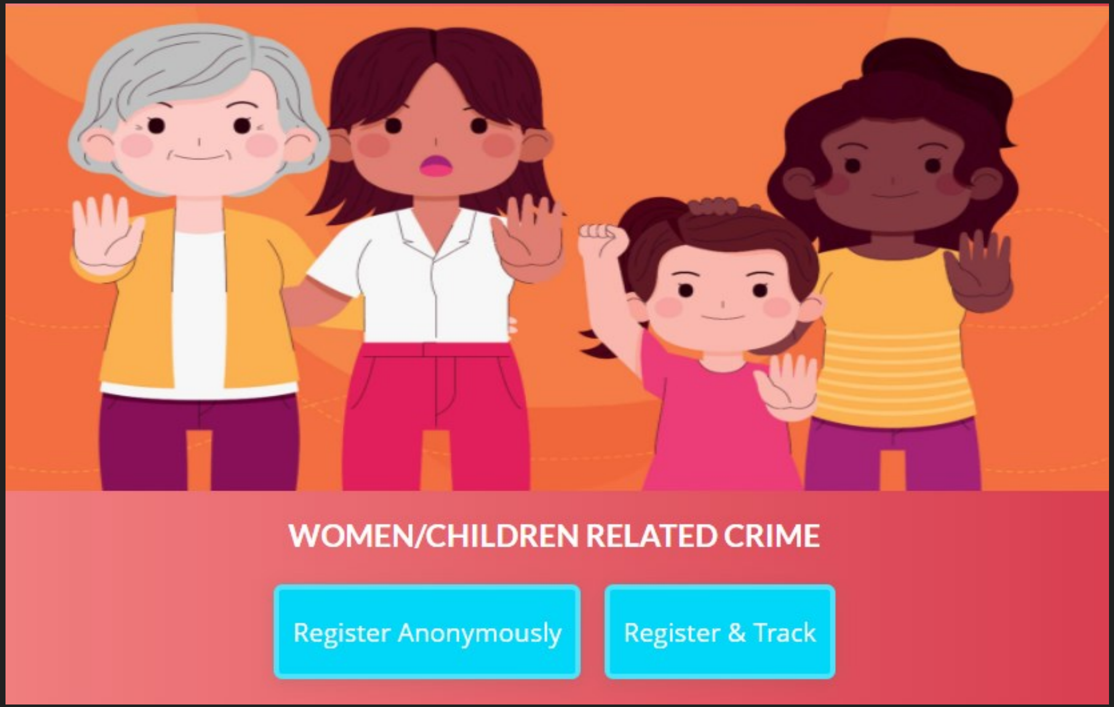
Child Pornography/Child sexually abusive material

Child sexually abusive material (CSAM) refers to material containing sexual image/video in any form, of a child who is abused or sexually exploited.

Reporting of Women / Children related Cyber Crime

cybercrime.gov.in

- Report Anonymously
- Report and Track
    - Login with Mobile number


WOMEN/CHILDREN RELATED CRIME

Awareness creation by GOI in Cyber domain.

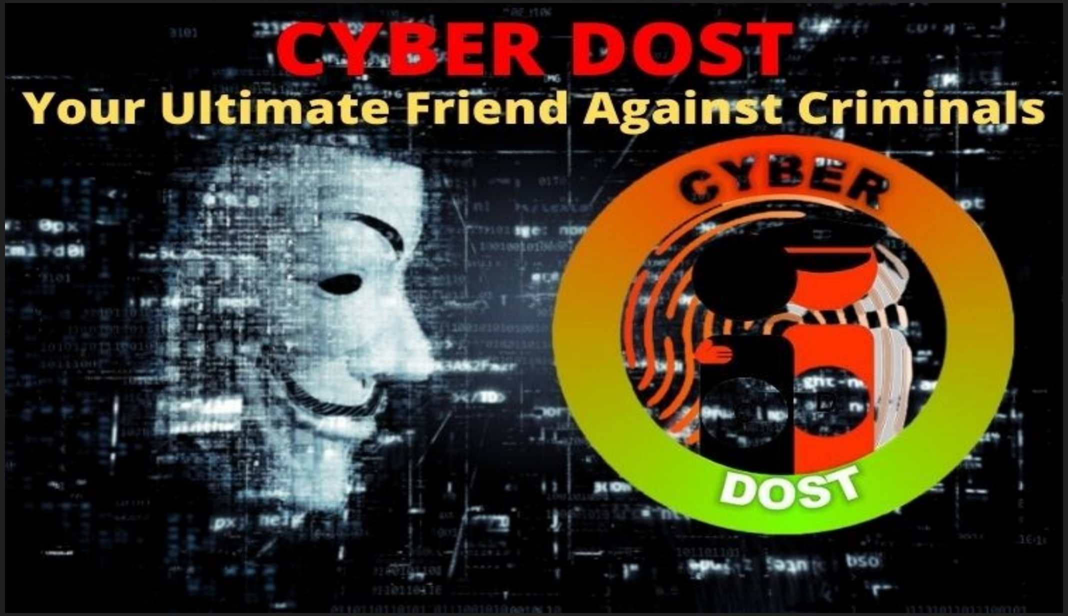
- To spread awareness on cybercrime, MHA has taken several steps that include dissemination of messages on cybercrime through:

➢ Twitter handle @cyberDost,

➢ Cyber Jagrookta Mission

➢ Radio campaign, TV campaigns

➢ Social Media handles of Cyber Crime Division Punjab



Where do threats arise from?

- Webcams/cameras
- From social media
- Physically meeting online acquaintances
- Leakage of documents from the digital devices
- Through spywares and malicious software.

Cyber safety on social media DOs/DONTs

- Privacy
- Usage
- Device Safety

Cyber safety on social media DOs/DONTs

Privacy

1. Strengthen privacy settings.

2. Set strong passwords for your social media accounts.

3. Turn on 2-step verification.

Cyber safety on social media DOs/DONTs

Usage

1. Think before you post.
2. Try not to befriend strangers.
3. Do not click any unauthorized link.
4. Don’t meet online acquaintances alone.
5. Report and flag content that is abusive or illegal.

Cyber safety on social media DOs/DONTs

Device Safety

1. Never keep your devices unattended.
2. Keep backup your data.
3. Don’t leave your webcam connected.
4. Do not install freeware.
5. Keep browser, operating system and antivirus up-to-date.

Cyber safety on Financial Frauds

- Personal Banking Information
- Debit/Cards
- Online Shopping

Cyber safety on Financial Frauds

Personal Banking Information

- 1. Keep all your important documents safe and secure.
- 2. Never give out your personal details when you’re contacted by phone or email.
- 3. Never give your bank details to anyone unless you know and trust them.
- 4. Periodically change passwords of your online banking accounts.

Cyber safety on Financial Frauds

Debit/Cards

- 1. When using a credit or debit card, make sure it’s never out of your sight.
- 2. Guard your card and details when making a transaction
- 3. Don’t write down information like PINs, passwords or logins.
- 4. Report any transactions you don’t recognize, even small amounts.

Cyber safety on Financial Frauds

Online Shopping

- 1. Get to know the seller/buyer - if possible, check the auction website for feedback on this person.
- 2. Never put your banking information on lesser known shopping websites.
- 3. Don't enter a password when someone is sitting beside you as they may see it.
- 4. Always remember to log off from your online bank portal if used for payment.

Prevalent Financial Frauds

- Drugs in Parcel Fraud
- Trading & Investment fraud
- Work from home Fraud

Drugs in Parcel Fraud

- Scamster calls posing as a courier staff
- Claims that drugs found in parcel in your name enroute to some foreign country.
- Parcel seized by the customs department with your Aadhaar card details.
- Later scammers posing as customs officials and as senior police officers contact their targets over the phone (VOIP calls)
- You will be asked to deposit huge amounts of money in order to get your name cleared and avoid any criminal proceedings

Trading & Investment fraud

- Victims contacted by scammers on social media channels like WhatsApp or Telegram, with offer of lucrative investment opportunities.
- They are asked to invest in trading / crypto platform, for which they usually receive returns in the beginning when small amount invested.
- After boosting their confidence and scam will ask them to investment more.
- The scammers add the victims to a Telegram group / Whatsapp Group where they create fake, sophisticated, and unique-looking crypto trading platforms and fake members talking about their huge gains.
- To further deceive victims, scammers create fake virtual crypto wallets on the website / Fake Apps to give the impression that their money is safe and secure.
- Victims are frequently caught up in this scheme, sending money on a daily basis and sometimes losing their entire life's savings.

Work from home fraud

- A message from scammer posing as human resource (HR) representatives from well-known companies.
- The job is to like, follow and comment on social media accounts and YouTube videos
- Victim assured of payment of money for each task assigned and some money is paid in the beginning to gain their trust.
- Victims are asked to send money and complete certain tasks in order to multiply their investment.
- Victims don’t get paid as some mistake is pointed out in their assigned task.
- In the end, victims are defrauded with lakhs of Rs.

What to do if you become a victim of Cyber Crime

- Contact the nearest cyber cell or police station, or
- File complaint through National Cyber crime Reporting Portal (cybercrime.gov.in)
- Identify the contact information/photo/video of suspects if any
- Block but don’t delete (provide the URLs and screenshots to police officer)

Thank
you!