Topic: Identity Theft:

1) Misuse of photocopies of identity proofs

- Never provide details or copy of identity proofs (e.g., PAN Card, Aadhaar Card, Voter Card, Driving License, Address Proof) to unknown person/organization.
- Be careful while using identity proofs at suspicious places.
- Do not share sensitive personal information (like Date of Birth, Birthplace, Family Details, Address, Phone Number) on public platforms.
- Always strike out the photocopy of the identity proof; write the purpose of its usage overlapping the photocopy. This way, it becomes difficult to reuse the photocopy.
- Do not leave your credit, debit or ATM card receipts behind, in places such as a bank/ATM or a store; never throw them away in public.

==========

Topic: Psychological Tricks:

1) Job Related Fraud:

- Always search and apply for jobs posted on authentic job portals, newspapers etc.
- Check if the domain of the e-mail is the same as the one you have applied with. For example, all government websites have ". gov.in" or ".nic.in" as domain.
- If an e-mail has spelling, grammatical and punctuation errors, it could be a scam.
- Beware of the fake calls/e-mails impersonating themselves as recruiters and requesting for personal information or money.

==========

Topic: Social Media Frauds:

1) Sympathy Fraud:

- Be careful while accepting friend request from strangers on social media. Cyber criminals often create fake social media profile to befriend potential victims with an intention to harm them.
- Do not share personal details or get into financial dealings with an unknown person whom you have met on social media platform.
- Keep family/friends informed, in case you plan to meet a social media friend. Always plan such meetings in public places

2) **Romance Fraud:**

- Be cautious while responding to unknown friend requests on social media platforms. Do not respond to unknown friend requests.
- Never share intimate pictures with anyone on online platform as they can be misused later.
- Do not share personal details or get into financial dealings with an unknown person whom you have met on social media platform.

3) **Cyber Salking:**

- Restrict access to your profile. Social media sites offer privacy settings for you to manage who can view your posts, photos, send you friend request etc.
- Ensure your personal information, photos and videos are accessible only to your trusted ones.
- Be careful while uploading your photos on social media which show your location or places you frequently visit as cyber stalkers may keep tabs on your daily life.

4) **Cyber Bullying:**

Be careful:

- If your child's behaviour is changing and he/she is more aggressive than before and If suddenly your child stops talking with you or his/her friends.
- If he/she stops using digital devices or is scared.
- Make your children aware that cyber bullying is a punishable crime so that neither do they indulge themselves in cyber bullying nor do they let anyone tease them.
- Discuss safe internet practices with your friends and family regularly.
- Monitor your kid's activity on internet/social media. Enable parental controls on computer/mobile devices.
- Even if the children or students know about any friend who is a victim of cyber bullying, they should help the victim. Report the matter to parents or teachers immediately.
- Do not delete offensive messages as it will help the police in investigation.