1 Only accept friend requests from people you know.

2 Go through your friend list regularly and remove the people you are not friends with anymore.

3 Do not click on suspicious links on your posts and messages that can give access to strangers to your account.

4 Do not give out full names, date of birth, and location of children on Facebook as it becomes an easy target for identity theft.

5 Set strong privacy settings by going to Settings>Privacy. See to it that your profile is private and your posts are only accessible by friends.

6 Turn off your location before posting on your feed.

7 Report spam or abuse whenever you come across profiles who send unwanted messages or comments on your posts.

8 Create separate groups for close friends and family and make sure you only post content about your child on those groups.

9 When memories related to your child shows up on Facebook or any other apps, and if you wish to share, always remember to share only on those specific groups that you have vetted already and not with everyone in general.

10 Be careful to share photos on messenger. Share only with people you know.

11 Create a different email for your Facebook. This would ensure that your account is not easily accessible through your mail.

12 Activate Two Factor Authentication by clicking the three-dot menu and going to Settings>Security and Login>Two Factor Authentication>Authentication app or SMS.
This will ensure that you have maximum safety on your Facebook Account and for someone to hack they need to be present near your device.

13 It is now easy to share content easily through all three of these social media - WhatsApp, Facebook, and Instagram. Make sure you post wisely as your data can end up on either of these apps easily.

14 Pubic accounts such as School handles should make sure they upload photos of children cautiously since data can easily be accessed when posted publicly.

1. Control your privacy settings. Tap on the three-dot menu and go to Settings>Account>Privacy. You can change who can view your profile photo and the information you share. This would prevent leaking of personal photos to unwanted people.

2. You can change your privacy settings on your status by going to Settings>Account>Privacy>Status>Only Share with.
   By selecting this option you can share content about your children only with people you want and not everyone on your contacts.

3. Block Unwanted users on your WhatsApp by going to Settings>Blocked Contacts.

4. Share photos and personal moments with only those you know.
   If you're sharing photos in groups make sure it is only with your friends and family.
   If you end up in a group that you do not know. Leave the group immediately.

5. Enable Two-Step Verification by creating a six-digit pin for extra security.

1. Enable Two Factor Authentication. You can find this by going to your Settings>Security> Two Factor Authentication. Two-factor authentication would assure that no one can access your account without having physical access to your device.

2. Check login activity. This page shows a list of locations from where you have logged in. If there are locations you have not logged from immediately log out from those. You can find it by going to Settings>Login Activity

3. Block and report accounts that post inappropriate photos and comments. You can do this by going to Settings>Privacy>Restricted Accounts. You can add username manually to block them.

4. Manage your tagged photos since anyone can tag you. You can remove yourself from these images by going to Settings>Privacy>Tags and turn off the tag feature automatically. You can also remove individual photos by finding an image and clicking on the three-dot menu, and then tap Hide Options(Android) or Photo Options(iOS).

5. Do not accept requests from strangers and keep your profile private.

6. Remember to set ground rules on sharing posts about your kid with your caregivers and your friends and followers on social media groups and pages.

Phone Privacy Settings

1. Check the privacy setting of your phone by going to Settings>Privacy. This varies from phone to phone.

2. For Android users please ensure to find Permissions Manager in your Settings and go through the kind of access you are giving to apps. Revoke access where you feel is not necessary.

3. You can also go to your settings and search for Special Access or App Management, and revoke different apps that access your data by revoking their usage access. This is a very good process to make sure you are not unknowingly giving out your data.

4. Check which apps can access your location on your phone by searching Location in your Settings. Find the apps that access your location and remove access for the ones that are not needed.

5. Be cautious and do not use free public WiFi because these networks are not secure and it is easy to get hold of your data for hackers.

6. Enable remote wipe on your phone. If you ever lose it then you will be able to remove data from the phone without it falling into the hands of strangers.