Cyber-security Advisory

Cyber Fraudsters are adopting many fraudulent tricks to defraud unsuspecting and gullible people.

'**Impersonation'** and '**Identity Theft'** are two very common ways for fraudulent activities.

Impersonation

Impersonation happens when someone pretends to be you. He/She may use social media to get information about you and then use that information to defraud you. For example, someone can copy photos of Top Management officials and create fake profiles. Then, those profiles are used in all kinds of communication with the subordinates to extract money. The communications can be in the form of Whatsapp messages, calls or even normal voice calls. The fraudsters take advantage of a normal human being's nature of listening to seniors in everyday office life. However, in the virtual world, it's always risky to trust without adequate verification.

To stay safe from Impersonation attacks, please do the following:

1. Check the origin of the communication. For example, check the country code.
2. Stop, Think and Act. Don't act immediately.
3. If in doubt, disconnect the communication and verify using a trusted channel of communication like a known phone number.
4. Beware of Unusual Requests, Urgent Demands, Unusual Offers etc.
5. Don't click on untrusted links.

Identity Theft

Identity Theft happens when someone steals your personal information and uses it to access your financial accounts and Social accounts etc. For example, personal information like your name, address, date of birth, Aadhaar number, credit card number, bank login credentials etc. are stolen and used to defraud you.

To stay safe from Identity Theft, please do the following:

1. Handle sensitive information carefully. Do not put sensitive information in email, social media, or text messages.
2. Make sure that you're using the correct website.
3. Create strong passwords and keep them secret.
4. Enhance your computer's security.
5. Do not use untrusted WiFi connections.

Stay cyber-safe.