Cyber-security Advisory

Cyber Fraudsters are using Impersonation as a tool for fraudulent activities. For example, they are copying photos of Top Management officials and creating 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.

Stay cyber-safe