## Beware of Job Offers / Investment Schemes with high returns that appear Too Good to be True.

- Money transfer agents, also known as money mule, are individuals who offer their bank accounts for use by fraudsters to transfer funds via the internet.
- Fraudsters typically post seemingly legitimate job postings on the internet, messaging platforms or via SMS, offering a commission for using an applicant's bank account. Little does the responsible person realise that such behaviour may result in criminal charges such as money laundering or ponzi scheme fraud.
- The advertisement may ask for people who have accounts with specific banks, particularly those that offer online banking and/or UPI.

## You can avoid becoming a money mule by doing the following:

- Be wary of any unsolicited offers or opportunities offering you easy money or jobs with work from home and flexi time. Do not participate in bids for lending your bank account to strangers.
- Fraudsters send appealing offers via email, phone calls, and SMS messages, asking you to deposit money to participate in schemes that appear too good to be true. They later withdraw the money and cease all communication.

## The following is a list of the most common types of fraud:

- Phone calls or SMS messages from a foreign country requesting personal information, offering jobs that you have not applied for, intimation, or gifts.
- Check the credentials of high return investment schemes and multilevel marketing schemes that offer high returns on investment in a short period of time.

## **Remember These:**

- Be wary of online scammers attempting to obtain your personal information. Avoid being a victim of phishing.
- Always enter the website address. Clicking on links should be avoided because they may lead to fraudulent websites.
- Do not enter sensitive information into any window that may appear while conducting an online financial transaction.
- Do not open e-mails or attachments from people you do not know.
- Do not fall victim to online investment schemes that promise higher returns or money doubled; such schemes are typically fraudulent.
- Never respond to any email requesting that you confirm, upgrade, renew, or validate your account information.
- Never give out your OTP, date of birth, card PIN, or personal information to anyone.