Warning signs

- Unsolicited communications claiming to originate from banks, government agencies, law enforcement authorities, or other trusted organisations.
- Requests for personal information, banking credentials, passwords, PINs, or OTPs.
- Messages creating a sense of urgency, fear, or pressure to make immediate payments or disclose sensitive information.
- Requests to transfer funds to personal bank accounts, digital wallets, or accounts unrelated to the purported organisation.
- Instructions to install unfamiliar applications or grant remote access to electronic devices.
- Online relationships that rapidly progress to requests for financial assistance, gifts, or investments.
- Emails, text messages, or social media communications containing suspicious links or attachments.
- Requests for advance payments to secure loans, prizes, inheritances, employment opportunities, or the release of funds.
- Inconsistencies in the identity, contact details, or explanations provided by the person or entity making the request.

Measures you can take to protect yourself,

- Refrain from installing or downloading applications from unverified sources
- Avoid granting third parties access to personal devices
- Ensure OTPs or any multi-factor authentication measures are not easily retrievable by unauthorized parties.
- carefully verify the URL of websites before logging in.
- Set up real-time SMS or email alerts for all types of transactions to immediately detect unauthorized activity.
- Avoid clicking links in unsolicited SMS or email messages and to manually type the URL of the website into the browser.
- Ensure that personal bank accounts are maintained and operated exclusively by the account holder and are not made available for use by third parties.

If you believe you have been affected by such a scam,

Do:

- If a person believes that they have been affected by a scam, they are required to immediately lodge a complaint at the nearest police station and report the same to the Financial Intelligence Unit with the relevant details including the account number to which the money was deposited/ said to be deposited, name of the account holder, relevant bank, mobile phone number where the information was received and the screenshots of the relevant messages via fiu@cbsl.lk

Don't:

- Avoid deleting proof of communications had with the scammer/ fraudster including messages, emails, transaction records, screenshots, or other relevant evidence.
- Refrain from using the same passwords on affected accounts.