Observations of Anti-Deception Coordination Centre ("ADCC")

ADCC has identified two prevalent causes of WhatsApp hijacking:

1. Failure to log out from WhatsApp Web, leaving active sessions vulnerable; and

2. Clicking suspicious hyperlinks contained in phishing SMS messages that redirect users to fraudulent websites designed to capture verification codes.

Recommended Preventive Measures

To mitigate such risks, ADCC recommends the following security practices:

1. Regularly check and log out from linked devices after use.

2. Enable two-step verification to enhance account security.

3. Never disclose verification codes to anyone.

4. Avoid interacting with suspicious links or downloading attachments from unknown emails, SMS, or websites.

5. Refrain from submitting sensitive personal or financial information, including personal information, credit card details, CVV codes, or one-time passwords, to unverified platforms.

6. Use the "Scameter+" tool to check suspicious URLs and consult relevant authorities.

7. Rigorously cross-check payment receipts and bank account records to confirm that funds were deposited or transferred correctly.