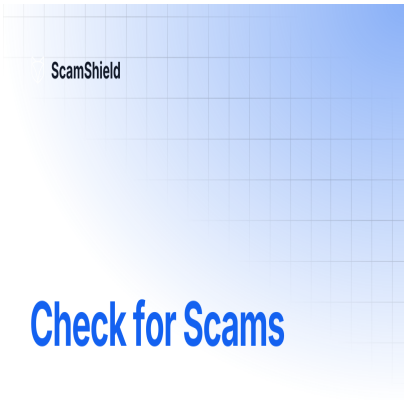

â??Likely-SCAMâ?• SMS: What the Sender ID Label Does and Does Not Prove

Description

default watermark

Since 31 January 2023, unregistered alphanumeric and relevant numeric Sender IDs sent to Singapore mobile users are relabelled â??Likely-SCAMâ?•.

A registered Sender ID reduces spoofing risk but does not prove every message or link is safe.

Read the label narrowly

Likely-SCAM means the sender ID was not recognised under the registry route; it is a strong warning, not a judicial finding about the person behind the message. Delete or report suspicious messages only after preserving what the bank or police may need. (SGNIC SMS Sender ID Registry overview)

A registered name can still be used in a socially engineered message sent through a compromised account or followed by a separate call. Verify the transaction or notice inside the official app rather than tapping the SMS link.

Situation	What changes
Message is labelled Likely-SCAM	Do not use its link or number; verify independently
Sender name looks familiar	Still verify any unusual request
Message asks for password, OTP or transfer	Stop and contact the organisation through its official app or website
Organisation sends customer SMS	Register every exact sender format and use a participating aggregator

Related: add a second-channel family verification rule

Check exact formatting

SGNIC warns that sender IDs are case sensitive. An organisation that registers one capitalisation and sends another may see messages blocked or relabelled. Businesses should inventory production, test and vendor sender strings before launch. (SGNIC SSIR FAQs)

Only participating aggregators can handle registered IDs under the regime. Vendors may need a Letter of Authorisation and must route through the approved chain. A marketing vendorâ??s assurance is not a substitute for checking the registry arrangement.

Example: An SMS appears under a bankâ??s familiar registered name but asks for an urgent account-verification transfer. The name alone does not validate the request. Close the message and check the bankâ??s official app or card hotline.

Allow registration lead time

SGNIC says the full process typically takes about 19 calendar days when documents and payments are prompt, and payment notices have 30-calendar-day deadlines. Build registration into the campaign plan instead of attempting it on launch day.

default watermark

Open the organisationâ??s official app, type its known website address or call the number printed on a physical card. Never search for a hotline using words supplied by the suspicious message because paid or manipulated results can mislead.

Related: spot another impersonation route

Date Created
09/08/2026
Author
claratan