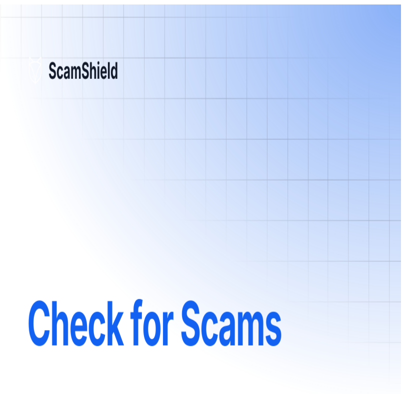

How to Check a Suspicious Message With ScamShield

Description

Do not tap, reply or call the number in the suspicious content. Open ScamShield separately, use the check feature and paste the message text or upload a screenshot. The result is a risk signal, not a guarantee: urgent requests for money, credentials, app installation or account access should still be verified through the organisationâ??s independently found official channel.

This guide is for a singapore resident who has received a suspicious message, call or link. It resolves one practical task: check the content without interacting with it and choose the right next action. It is desk-reported from the two cited primary sources and does not claim a field visit or professional advice.

Use this decision table first

Fact pattern	Practical result
You only received a message	Preserve it and check text or screenshot in ScamShield
You tapped but entered nothing	Close the page, check device permissions and verify the claimed sender
You entered credentials	Change them through the real service and secure linked accounts
You transferred money	Contact the bank immediately, then Police and 1799
Threat or safety risk is unfolding	Call 999 rather than waiting for a content check

Capture evidence without forwarding risk

Take a screenshot showing sender, date, message and URL text. Do not open the link merely to make the evidence clearer. Forwarding a live link to family can spread the hazard, so share an image or describe the domain instead. The controlling reference is [ScamShield check for scams](#).

Use the checker from a trusted starting point

Launch the installed ScamShield app or type the government address yourself. Paste message text or upload the screenshot. A scammer can imitate a result page, so do not follow a link inside the suspicious message that claims to lead to ScamShield.

Read the result as one input

Automated and community signals can identify known patterns, but new campaigns evolve. A low-risk or inconclusive result does not authenticate the sender. Verify invoices, delivery notices, bank alerts and agency requests using contact details from the real app, card or official website.

Match the response to what was exposed

If nothing was clicked, blocking and reporting may be enough. If credentials, card details, Singpass data or a one-time password were entered, secure the affected account immediately. If an app was installed, disconnect the device and obtain technical help before using it for banking. Cross-check the operational detail against [ScamShield message-check guide].

Escalate money movement first

When a transfer or card payment has occurred, minutes matter. Call the bank through its official number to freeze or recall transactions, then make the appropriate Police report. The 1799 ScamShield helpline operates around the clock for scam guidance, but it does not replace an emergency call.

Report enough context to help others

Submit the message, sender and screenshots through ScamShield without adding invented conclusions. Preserve bank references and the website address. Accurate reporting improves investigation and detection while keeping a clean chronology if the victim later disputes a transaction.

A worked decision

A parcel message says a S$1.20 fee is due and links to a lookalike domain. The recipient screenshots it, checks the text in ScamShield and independently opens the courierâ??s official app. No fee appears, so the message is blocked and reported. If card details had already been entered, the first priority would instead be the card issuer.

Complete these checks in order

1. Stop interacting with the message or caller.
2. Screenshot the sender, content and visible URL.
3. Open ScamShield independently and run the check.
4. Verify the claimed organisation through its real app or website.
5. Secure every credential or payment method that was exposed.

6. Call the bank and Police promptly if money moved.
7. Block and report with an accurate evidence record.

For other current public-service tasks, see our public-transport savings guide and Climate Vouchers spending guide. Those pages answer distinct downstream questions and do not replace the authority rules cited here.

Common mistakes to avoid

- Tapping the link to inspect it
- Calling a verification number supplied by the sender
- Treating an inconclusive result as proof of safety
- Changing only one reused password
- Waiting for a checker result after money has moved

Keep a dated file containing the source pages, submitted forms, approvals, signed agreement and calculations. Rules, service interfaces and temporary concessions can change. Recheck the authority page immediately before acting, especially when the transaction will occur after a published end date or involves an unusual use, payment or occupier.

Make the decision easy to revisit

Before acting, write down the date, the fact that determines the outcome and the source page used. For this question, the decision is whether to check the content without interacting with it and choose the right next action. The two practical tools aboveâ??a harm-based response tree separating receipt, click, credential exposure and money loss and a parcel-fee verification example that avoids touching the attackerâ??s linkâ??are intended to make that reasoning visible. Save the result with receipts, confirmations or screenshots generated by the official service. If a deadline, amount, status, traveller, employee, property or health circumstance changes, rerun the decision from the beginning instead of editing the old answer from memory. Where a professional adviser, agency officer or service provider gives a different answer, ask which current rule and which facts produce the difference. That short record is valuable when two family members, colleagues or counterparties otherwise remember the same conversation differently.

Questions readers ask

Can ScamShield check a screenshot?

Yes. Its guide explains that a screenshot can be uploaded, or message text can be pasted.

What is the ScamShield helpline?

Call 1799 for scam guidance; the service is listed as 24/7.

Should I call 1799 in an emergency?

For an immediate threat call 999, and for transferred money contact the bank without delay.

Primary references and limits

ScamShield check for scams and ScamShield message-check guide were checked on 17 July 2026. The article applies their published general rules to the examples above. It does not determine an individual application, resolve a contractual dispute or replace legal, tax or regulated advice.

Date Created
17/07/2026
Author
claratan