



Courier Phishing Scams: How the S\$1 Redelivery Trap Works

Description

Do not pay a tiny redelivery fee from an unsolicited message. Police said on 15 July that at least 43 cases had been reported since 24 June, with losses exceeding S\$259,000. The trap moves from a fake S\$0.06 to S\$1.64 fee into card capture and a mobile-wallet approval.

Start with the decision table

Situation	What it means
No parcel is expected	Delete the message and do not test its link
A parcel is expected	Open the merchant or courier app independently
Page says the address is incomplete	Check the order record, not the message's prefilled details
Wallet asks to add a card or approve a device	Cancel; a redelivery fee does not require wallet enrolment
Card details were entered	Call the bank immediately, block the card and report

The small amount lowers suspicion

[SPF courier phishing advisory, 15 July 2026](#) describes fake fees between S\$0.06 and S\$1.64. The criminal objective is not the fee; it is the card and authentication flow. Treat any payment page reached from an unexpected delivery message as untrusted.

The address deadline creates pressure

The message may claim an incomplete address and a 24-hour deadline. Real urgency does not make a supplied link safe. Close it, open [SingPost mobile app](#) or the merchant's saved order, and enter the tracking number independently.

A mobile-wallet prompt is the pivot

Police says victims were led to add cards to mobile wallets. Read every bank notification literally: adding a card or approving a new device is not the same as authorising a one-dollar delivery charge.

Email sender names are easy to imitate

The advisory notes random email addresses and courier impersonation. A familiar logo, parcel vocabulary or matching first name is not proof. Inspect the domain and use a channel already saved on the phone.

Act in the right order after exposure

First call the bank and block affected instruments. Then change reused passwords, review wallet and device enrolments, preserve the message and report through ScamShield or Police. Do not keep clicking to collect evidence.

Worked application

The loss pattern shows why the fee is camouflage: S\$259,000 divided by 43 cases is more than S\$6,000 per case on average, using the advisory's minimum figures. That is a lower-bound calculation because Police said "at least" 43 and "more than" S\$259,000.

Action checklist

1. Do not open the supplied link
2. Check the order in a known app or typed domain
3. Read bank prompts for card-add or device-enrolment language
4. Cancel any unexpected wallet action
5. Call the bank immediately after disclosure
6. Preserve the message and transaction evidence
7. Report and warn affected household members

Build a decision record another person can check

The useful output is not only an answer to "courier phishing scam Singapore?". It is a small file showing why the answer fits this reader: a singapore resident receiving an unexpected parcel or redelivery message. Record the fact that controls each step, the date it was true and the source or service that confirmed it. That matters because the task is to stop the scam path before entering card details or approving a mobile-wallet prompt; a changed amount, date, person, address, venue, device or eligibility fact can change the result even when the general rule has not moved.

#	Control	Evidence to retain	Failure signal
---	---------	--------------------	----------------

1 Do not open the supplied link	Authority page or service readback	Paying because the amount is tiny
2 Check the order in a known app or typed domain	Dated input, statement or booking screen	Trusting a logo or sender display name
3 Read bank prompts for card-add or device-enrolment language	Calculation sheet with assumptions	Approving a wallet prompt to finish checkout
4 Cancel any unexpected wallet action	Written confirmation from the responsible party	Calling a number inside the message
5 Call the bank immediately after disclosure	Receipt, acknowledgement or reference number	Revisiting the phishing page after blocking the card
6 Preserve the message and transaction evidence	Photograph, timetable or versioned document	Paying because the amount is tiny
7 Report and warn affected household members	Final outcome and date checked	Trusting a logo or sender display name

The record should be short enough to update. Put the most recent evidence first, keep the earlier version, and label estimates separately from confirmed figures. The two original tools in this guide—a five-stage scam-path map from S\$1 fee to wallet enrolment and a lower-bound per-case loss calculation exposing the small-fee camouflage—serve different purposes: one structures the choice, while the other tests the choice against a concrete case. Neither should be copied into a new case without refreshing its inputs.

What each authority source establishes

Source	Claim used here	Freshness control
SPF courier phishing advisory, 15 July 2026	43 cases, more than S\$259,000 lost, email pattern, fake fees and wallet prompts.	Checked 2026-07-17; re-open before acting
SingPost mobile app	Official parcel tracking and delivery-management channel.	Checked 2026-07-17; re-open before acting

These links are attached to the claims they support, not offered as a substitute for explanation. If a service screen, signed agreement or officer's written response conflicts with the general page, preserve both and ask which fact or newer rule produces the difference. Do not conceal the conflict by selecting the more convenient answer.

For the adjacent decision, continue with our [suspicious-message check](#) and [OneService reporting guide](#). Each answers a separate next-step question.

Errors that change the outcome

- Paying because the amount is tiny
- Trusting a logo or sender display name
- Approving a wallet prompt to finish checkout
- Calling a number inside the message

- Revisiting the phishing page after blocking the card

Keep the dated authority pages, calculation inputs, confirmations and any advice used for the decision. This article applies public information to a general fact pattern and does not determine an individual application, contract, tax position, medical need or legal dispute. Recheck the linked primary source immediately before acting, especially where the transaction, journey, booking or filing occurs after a stated change date.

Questions readers ask

What was the reported scale?

Police said at least 43 cases and more than S\$259,000 lost since 24 June 2026.

How do I check a real delivery?

Use the merchant or courier app and tracking page opened independently.

What if I entered card details?

Contact the bank immediately, block the card and review mobile-wallet and device enrolments.

Date Created

18/07/2026

Author

claratan