carousell

2025 Regional

Scam Trends Report

How Carousell fights fraud across Greater Southeast Asia

Contents

3 Introduction

4 Scams keep evolving and we continue to fight back

5 Advancing the fight against scams at scale: How Carousell protected millions in 2025

8 Scam types observed in 2025

12 What we're doing to combat scams

13 What you can do to keep safe

Introduction

Fighting scams. Protecting users. Strengthening trust.

This report follows our 2024 edition, covering Singapore, Malaysia, Hong Kong, the Philippines and Taiwan, with the aim to raise awareness on new scam tactics and how to keep safe with both our safety measures and personal vigilance.

Key findings

Carousell's effort in fighting scams

99.96%
of transactions proceeded without scam incident

Over 93%
of active users did not encounter a scammer

451,000+
suspicious accounts suspended

520,000+
community reports investigated

More scam types observed

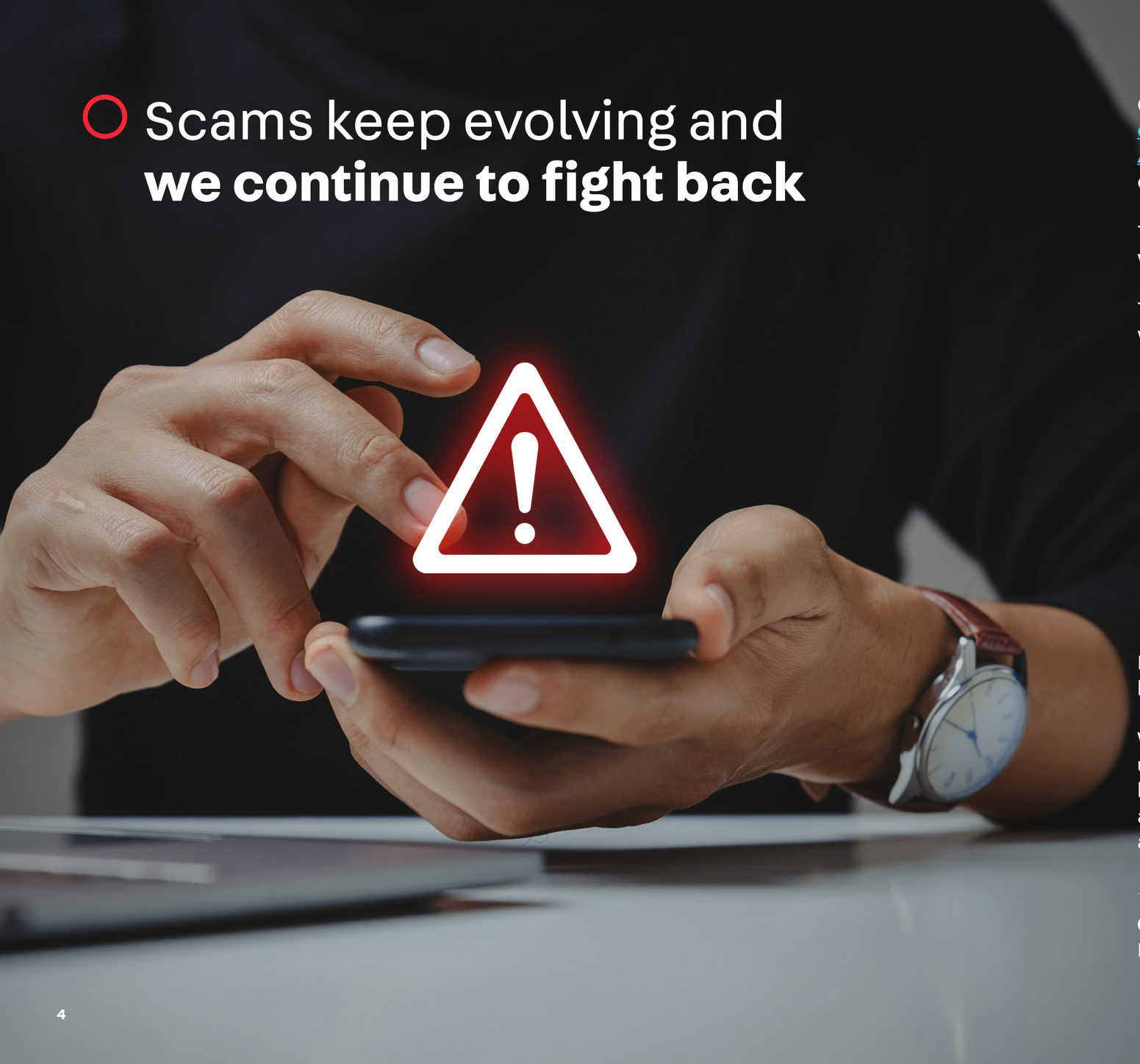
- **Ongoing scams with evolving tactics:** Off-platform phishing (fake payment) and the Philippines-specific 'Abono' scam.
- **New scams spotted:** Deposit-based scam, digital goods fraud, misrepresentation scam, and refund scam.

How scammers operate:

Scammers exploit urgency, impersonation, and off-platform chats to build trust quickly and pressure users into sharing personal information or making payments.

Prepared by Carousell Trust Working Group (April 2026)

Scams keep evolving and **we continue to fight back**



Online scams are constantly evolving, not just on Carousell but across every digital platform. Scammers have swiftly adopted the use of AI to create highly convincing scenarios, impersonate brands, and conversations to trick victims.

They innovate as quickly as platforms do. As their tactics level up, we must level up too.

That's why trust and safety isn't a one-time effort. It's something we work on every day at Carousell. Our approach includes:

1. Proprietary AI tools to detect scams, block harmful content and flag suspicious accounts.
2. Identity verification to prevent impersonation and account takeover, using measures like risk-based SMS checks.
3. Safer ways to transact, including built-in payment and delivery, verification measures, and safeguards tailored to the unique problems users face in each category and market.
4. Community education, user reporting tools and partnerships with trusted organisations.

But no system can stop scams alone. Scammers succeed when users bypass built-in warnings or move off-platform.

We are sharing the new edition of the report to provide the 2025 update on the latest scam tactics, helping you understand more on how scams work, how new methods are emerging, how to spot them, and how Carousell is staying one step ahead so you can stay safer and better informed.

Gijs Verheijke
Director of Trust and Customer Experience, Carousell

Advancing the fight against scams at scale: **How Carousell protected millions in 2025**

99.96% of transactions proceeded without scam incident

Key markets at a glance:

- **99.97%** Singapore
- **99.95%** Malaysia
- **99.95%** Hong Kong
- **99.93%** Philippines
- **99.99%** Taiwan

Based on recorded scam cases out of total transactions in 2025

These outcomes are achieved through the collective efforts of platform security, community vigilance, and user education.

Additionally,
over 93% of our active users across all markets did not encounter a scammer.

Proactively stopping risky activity

As sharing links, emails and QR codes have a high incidence of use for phishing scams and no crucial need in transacting, we restrict the sharing of such content for speed in prevention.

Breakdown by market:

All markets

740,000+ links restricted

364,000+ email addresses blocked

61,000+ QR codes intercepted

Malaysia

57,000+ links restricted

44,000+ email addresses blocked

4,600+ QR codes intercepted

Singapore

157,000+ links restricted

178,000+ email addresses blocked

15,000+ QR codes intercepted

Taiwan

54,000+ links restricted

7,700+ email addresses blocked

3,200+ QR codes intercepted

Hong Kong

124,000+ links restricted

92,000+ email addresses blocked

28,000+ QR codes intercepted

Philippines

54,000+ links restricted

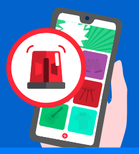
29,000+ email addresses blocked

2,800+ QR codes intercepted

We observed a decrease in links and emails blocked, but an increase in QR code interceptions compared to 2024. **This is likely due to two factors:**

A Scammers switching tactics to QR codes because they cannot send links and emails.

B Enhancement of our detection capabilities to identify and block such attempts.



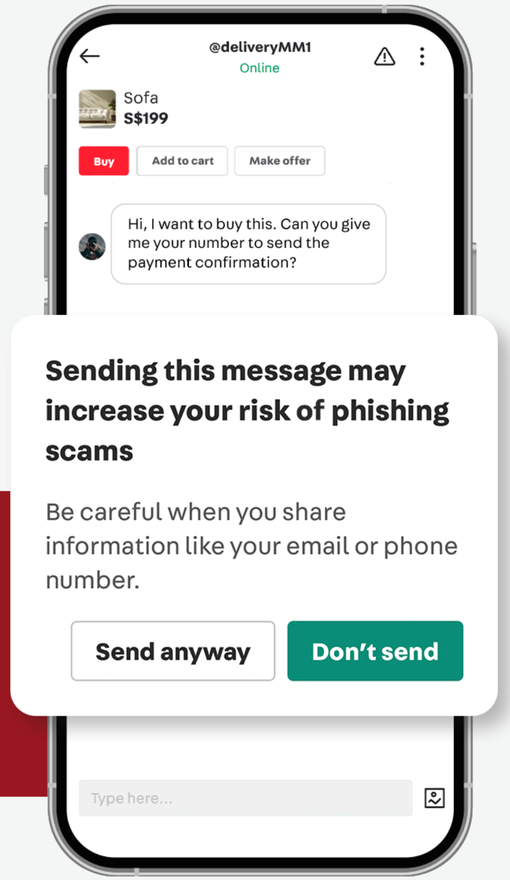
We have also seen scammers guessing email addresses from usernames to send phishing emails. **– Gijs Verheijke**

Preventing off-platform scams

We have seen a rise in scammers tricking users to chat or transact off platform. We have further increased friction in exchanging phone numbers via a pop-up warning with a button for users to proceed to share their phone numbers.

Out of 18+ million safety alerts shown,

83% of users still chose to share their phone number.



We understand from local police that phishing scam victims commonly share phone numbers in obfuscated ways to evade detection without realising it is a ploy by scammers. While we enhance our detection tools, we strongly urge users to follow our safety measures and consider potential buyers sharing their phone number in an obfuscated way to be a serious red flag. **– Gijs Verheijke**

Enforcement and community vigilance

Scammers often work at scale, so quick suspension of suspicious accounts can stop further harm. Our community also helps to look out for each other, and serve as early defence against new scam tactics.

451,000+
suspicious accounts detected.
Led to **424,000+** confirmed suspensions*

520,000+
community reports submitted.
Led to **306,000+** confirmed suspensions*

**While strict measures help keep Carousell safe, they may occasionally result in false suspensions. Legitimate users can appeal, and cases confirmed as false positives are used to retrain our models as we continue improving accuracy while maintaining strong scam protection.*

Data is based on Carousell's internal records from January to December 2025.

Scam types observed in 2025

While scam tactics evolve, the core objective remains the same: exploiting trust and urgency to convince users to pay upfront or move transactions off-platform.

Here are the scam types prevalent in 2025:

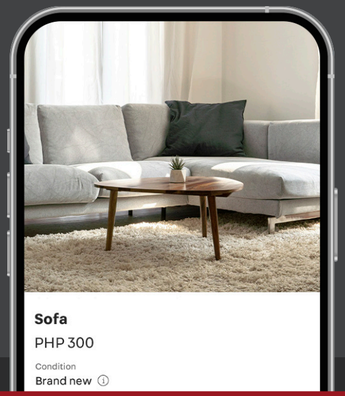
1 E-commerce scams (HK, MY, PH, SG, TW)

Scammers pose as legitimate sellers and offer attractive deals.

Deposit and pre-order (HK, SG, TW)

Scammers advertise high-demand or limited items, and need buyers to pay a deposit or full payment upfront.

Common with: Pokémon cards, K-pop merchandise, Event tickets, Toys and games, Audio products



Misrepresentation and non-delivery (MY, PH)

Scammers offer trendy or high-quality items at surprisingly low prices and appear friendly.

Common with: Men's and women's fashion, Furniture and home living

After payment, victims experience

- Shipping repeatedly delayed with excuses
- No tracking numbers or fake shipping updates
- Receiving defective or a different item than listed
- Seller becomes unresponsive or blocks the buyer

AI-generated images for illustration

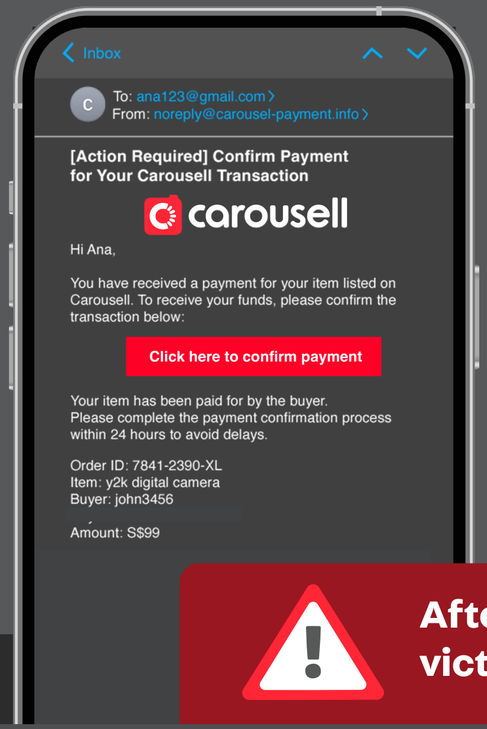
Here are the scam types prevalent in 2025:

2 Off-platform scams (HK, MY, SG)

Scammers often pretend to be buyers to move victims to a fake site to steal money.

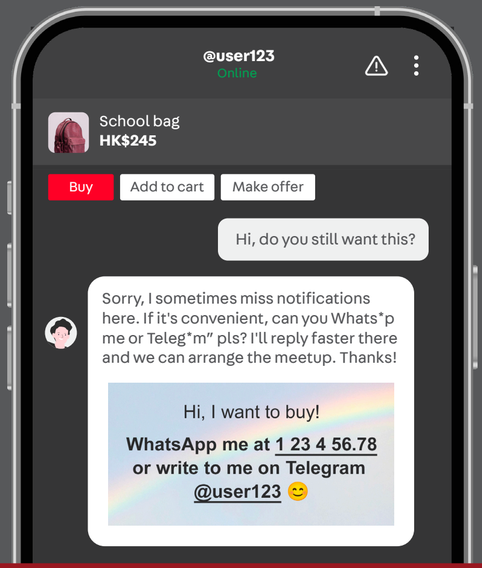
Phishing links (HK, MY, SG)

Scammers may ask for the user's email address and send fake links for 'payment confirmation'.



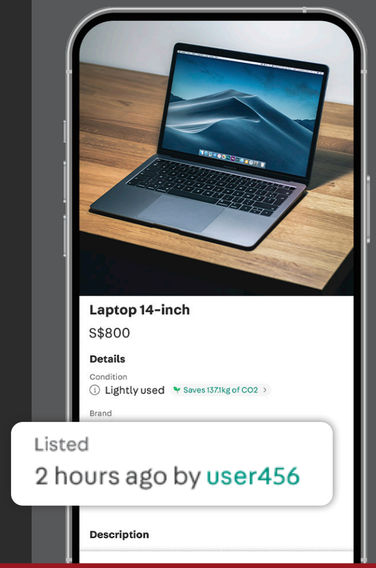
Phishing messages (HK, MY)

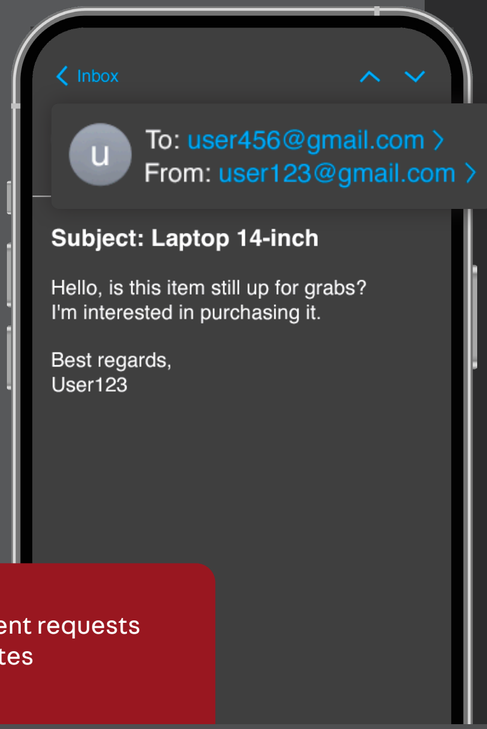
Scammers may suggest moving the conversation to WhatsApp or Telegram by using image or obfuscated text to bypass detection.



Email impersonation (SG)

Scammers guess email addresses based on Carousell usernames and send emails referencing actual listing titles to appear legitimate.





After engagement, victims experience

- Sharing personal details unknowingly
- Getting tricked into entering login credentials
- Approving fake payment requests
- Transacting on fake sites

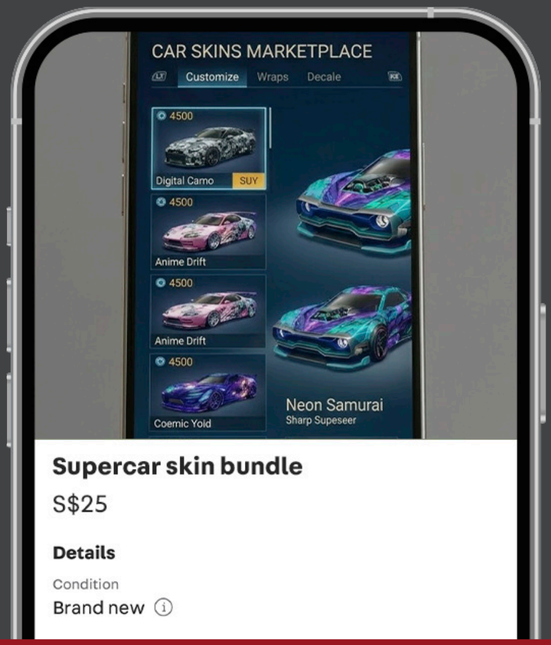
The examples provided herein are for illustrative purposes only. Any resemblance or reference to real persons, usernames, entities, or situations is purely coincidental, unintentional and are not intended to represent actual events.

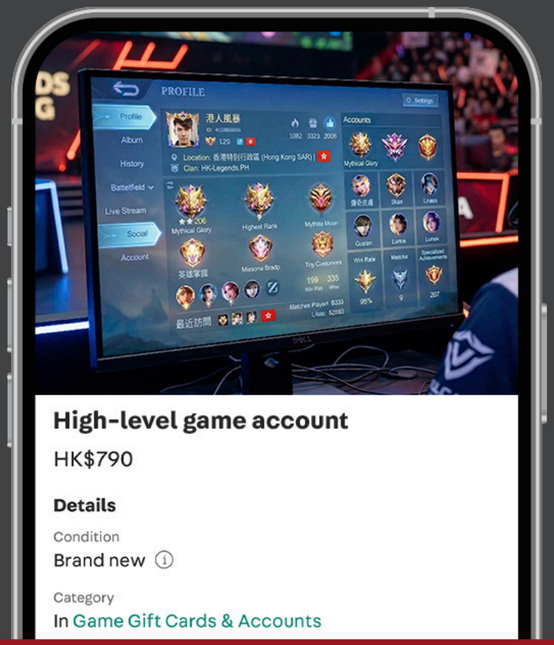
Here are the scam types prevalent in 2025:

3 Digital goods and gaming scams (HK, SG)

Scammers often target buyers of digital assets where transactions are difficult to reverse.

Common with:
Gaming gift cards, In-game items, Gaming accounts





After payment, victims experience

- Invalid, used or wrong region codes are sent
- Seller claims 'system delays', then disappears
- Seller disappears without giving account access

AI-generated images for illustration

Here are some prevalent scams spotted only in certain markets:

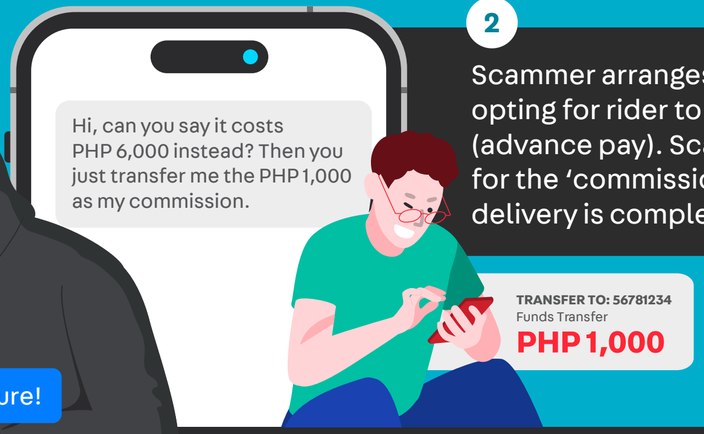
PH: 'Abono' scam

1

Scammer claims they are buying on someone's behalf and to mark up the amount as commission.

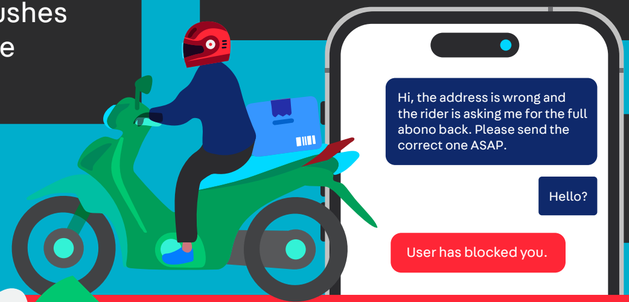
2

Scammer arranges for delivery, opting for rider to '*abono*' (advance pay). Scammer rushes for the 'commission' before delivery is completed.



3

Rider returns because the address is invalid and asks for their money back.



4

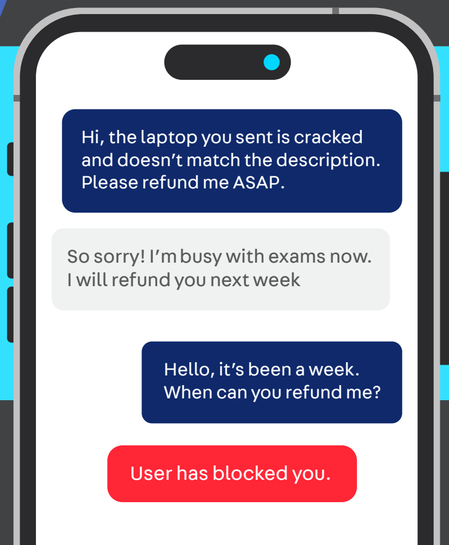
Scammer disappears.

Seller losses PHP 1,000 'commission' to the scammer and has to refund the rider's PHP 6,000 advance.

TW: Refund scam

1

Scammer delivers defective electronics or items that differ from what was listed.



2

They promise a refund to the buyer, but repeatedly delay with excuses and eventually disappear.

What we're doing to **combat scams**

We take a multi-layered approach to trust and safety to detect scam attempts early, reduce user risk, and take swift action when suspicious activity is found.

AI- and ML-powered detection and prevention systems

1

We use AI, machine learning (ML), and data science to detect suspicious actions across millions of daily interactions.

1	2	3	4	5
Ingestion	**Filtering**	**Analysis**	**Prevention**	**Human-in-the-Loop**
AI systems scan millions of listings, chat messages and account actions.	The data is processed through ML models trained on historical scam patterns.	ML models detect suspicious activity or patterns.	High-risk content, listings, or accounts are automatically restricted.	Human moderators may review cases for investigation and system refinement.

Account security and identity protection

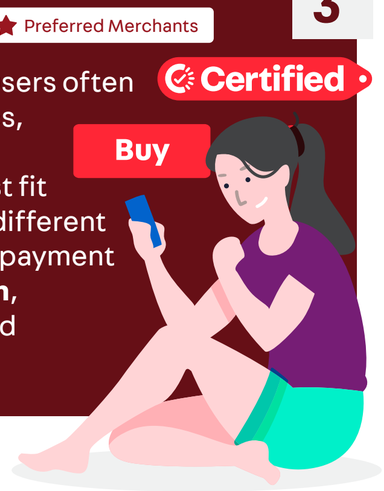
2

We continue to strengthen identity verification and login security to reduce impersonation and account takeover risks. A new measure added in 2025 to target high-risk login attempts is triggering SMS verification, instead of just email OTP.

Safer ways to transact

3

As a predominantly-C2C marketplace, users often handle payment and delivery themselves, which may have risks. We continually design trust-led models* tailored to best fit the unique problems users face across different categories and markets, such as official payment and delivery options via the **'Buy' button**, verified items via **Carousell Certified** and **Preferred Merchants** programmes.



*Programmes vary by region.

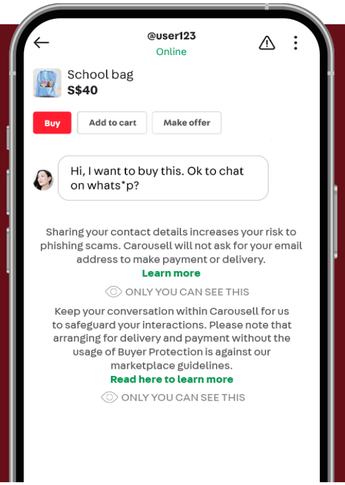


Image: In-chat prompt warning against sharing personal info or going off-platform.

User education and community reporting

4

We surface warnings within listings and chat windows tailored to the activity's risk profile. Users can also keep abreast of latest scam trends via monthly education campaigns. Our user community also serves as additional defense, reporting suspicious activity for investigation.

Partnerships with authorities

5

We work with authorities and trusted groups to fight scams, sharing insights and improving safety. These efforts help us better detect, prevent and respond to scams, so users can trade with confidence.

What can you do to **keep safe?**

While we work continuously to detect and prevent scams, staying safe also starts with being aware.

Carousell's Trust and Safety mascot

Here are some key steps you can take to protect yourself:

Keep all communication on Carousell

Scammers often move chats to WhatsApp or Telegram to avoid detection. **If someone insists on switching apps, it's a red flag.**

Be cautious of fake links and emails

Phishing scams often begin with fake emails or messages that appear to come from Carousell.

Report anything suspicious

If something feels off, report it. It helps protect others and your report stays anonymous.

Use Carousell's secure features where available

Use the 'Buy' button to pay after delivery, or meet in a safe place and check the item first.

Watch for e-commerce scam signs

Too-good-to-be-true deals, upfront payment requests, or rushed buyers are red flags. **Verify the listing or check with someone you trust first.**

Never share personal or payment information

Scammers may ask for your email, number, or bank codes. **Check your order details on your app's Profile page under 'Purchases' or 'Sales'.**

carousell

support.carousell.com