carousell | 旋轉拍賣

2025 年
詐騙趨勢報告

Carousell 旋轉拍賣如何打擊在香港、台灣及東南亞的詐騙行為

內容

前言
打擊詐騙、保護用戶、鞏固信任

本報告承接 2024 年版本，涵蓋新加坡、馬來西亞、香港、菲律賓及台灣，目的是提高大眾對新型詐騙手法的警覺性，並透過平台安全措施與用戶個人警覺，保障交易安全。

主要發現

Carousell 打擊詐騙工作

99.96%
的交易未有涉及詐騙

超過 93%
的活躍用戶未有遇到騙徒

封鎖了
逾 45.1 萬
個可疑帳號

調查了
逾 52 萬
宗用戶社群舉報

觀察到更多詐騙手法：

- **持續進行及演變的詐騙：**
  平台外釣魚詐騙（偽冒付款通知）以及菲律賓的「墊錢」詐騙
- **新型詐騙手法：**
  按金詐騙、數碼產品詐騙、虛假陳述詐騙以及退款詐騙

騙徒的操作手法：

騙徒會利用急切性、假冒身份及平台外通訊方式，快速博取信任，迫使用戶提供個人資料或進行付款。

報告編製單位：Carousell 防騙及交易安全工作小組（2026 年 4 月）

詐騙手法不斷演變，**我們亦持續應對**

網絡詐騙手法持續演變，不僅出現在 Carousell，也遍佈於各大數碼平台。騙徒已迅速利用人工智能（AI）製造高度逼真的情境、冒充品牌，甚至模仿真實對話內容，以誘騙受害者。

騙徒的手法與平台的發展同樣迅速。隨著詐騙手段不斷升級，我們亦必須不斷提升防範能力。

因此，增加買賣雙方的信任與用戶安全並非一次性的工作，而是 Carousell 天天都持續投入的重點。我們的防詐措施包括：

1. 自家研發的 AI 工具，用於偵測詐騙、攔截有害內容及標示可疑帳號
2. 透過風險評估式短訊驗證等措施，進行身份核實，防止假冒身份及帳號被盜用
3. 更安全的交易方式，包括內置付款及配送功能、驗證措施，以及針對各地市場及不同商品類別用戶面對的問題而設的安全保障
4. 推行用戶教育、舉報機制，並與可信機構建立合作關係

不過，沒有任何一套系統能夠全面阻止詐騙。當用戶忽視平台警告，或轉移至平台以外的渠道進行交易時，騙徒往往就有機可乘。

我們發布此最新版本報告，旨在提供 2025 年最新騙案手法的資訊，協助大家更了解詐騙的運作模式、新興行騙方法以及如何辨識相關風險。

同時，我們亦分享 Carousell 如何持續優化防詐策略，讓你使用平台時更加安心、更具警覺。

Gijs Verheijke
Carousell 信任與用戶體驗總監

大規模打擊詐騙：
Carousell 在 2025 年如何保障數百萬用戶的安全

99.96%

的交易未有涉及詐騙

重點市場概覽

- **99.95%** 香港
- **99.97%** 新加坡
- **99.95%** 馬來西亞
- **99.93%** 菲律賓
- **99.99%** 台灣

根據 2025 年總交易量中的已確認詐騙個案統計

這些成果有賴平台安全措施、
社群的警覺以及用戶教育三方面的共同努力。

此外，在我們所有市場中，
超過 93% 的活躍用戶均未有遇到騙徒。

主動遏止高風險活動

由於分享連結、電郵地址及 QR code 經常被騙徒用作進行釣魚詐騙，而且在平台交易過程中並非必要，我們已限制此類內容的分享，以更快速地預防相關詐騙行為。

各市場數據如下：

總計

- **740,000+** 已限制連結
- **364,000+** 已封鎖電郵地址
- **61,000+** 已攔截 QR code

台灣

- **54,000+** 已限制連結
- **7,700+** 已封鎖電郵地址
- **3,200+** 已攔截 QR code

香港

- **124,000+** 已限制連結
- **92,000+** 已封鎖電郵地址
- **28,000+** 已攔截 QR code

菲律賓

- **54,000+** 已限制連結
- **29,000+** 已封鎖電郵地址
- **2,800+** 已攔截 QR code

馬來西亞

- **57,000+** 已限制連結
- **44,000+** 已封鎖電郵地址
- **4,600+** 已攔截 QR code

新加坡

- **157,000+** 已限制連結
- **178,000+** 已封鎖電郵地址
- **15,000+** 已攔截 QR code

與 2024 年相比，我們觀察到被封鎖的連結及電郵數量有所下降，但被攔截的 QR code 則有所增加。這很可能與兩個因素有關：

A 騙徒因無法分享連結及電郵地址，而轉向使用 QR code 作為新的詐騙手法。

B 我們的偵測能力有所提升，能更有效識別並攔截有關企圖。

此外，我們在新加坡市場亦觀察到一種新手法：騙徒會嘗試從用戶名稱推測其電郵地址，並以此發送釣魚電郵。

– Gijs Verheijke

防範平台外詐騙

我們發現，誘導用戶轉到平台外聊天或交易的詐騙行為有上升趨勢。為此，我們進一步加強交換電話號碼的防範措施：當用戶嘗試分享電話號碼時，系統會彈出警告視窗，並提供按鈕讓用戶自行決定是否繼續分享。

在顯示的
1,800 多萬條安全警示中，

仍有 83% 的用戶選擇繼續分享自己的電話號碼。

管控與社群警覺

騙徒經常大規模作案，因此快速封鎖可疑帳號可防止更多用戶受騙。我們的社群亦會互相留意，充當對新型詐騙手法的重要防線。

451,000+
偵測到的可疑帳號
共封鎖超過 424,000 個違規帳號 *

520,000+
社群舉報提交
共封鎖超過 306,000 個違規帳號 *

* 嚴格措施有助保障 Carousell 平台安全，但偶爾可能導致誤封。正當用戶可就有關決定提出上訴，而經確認為誤判的個案將用作重新訓練我們的系統模型，讓我們在維持強效防詐保護的同時，持續提升識別準確度。

以上數據為 Carousell 內部統計，涵蓋 2025 年 1 月至 12 月。

根據各地執法機構的資訊，釣魚詐騙受害者常會以變形方式分享電話號碼，以規避系統偵測，卻未察覺這其實是騙徒的圈套。雖然我們不斷強化偵測工具，但仍強烈呼籲用戶遵守平台安全指引，並將買家以變形方式分享電話號碼視為重要警示訊號。**– Gijs Verheijke**

2025 年觀察到的詐騙類型

雖然詐騙手法不斷演變，其核心目標仍然不變：利用用戶的信任及過度急切的心理，誘使他們預先付款或將交易轉移到平台外進行。

以下為 2025 年常見的詐騙類型：

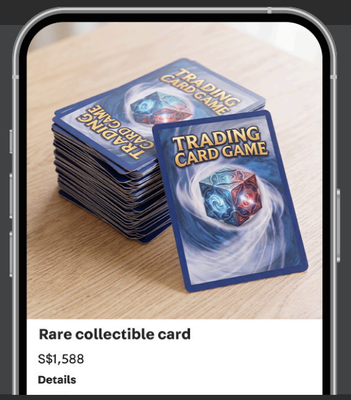
1 電商詐騙（香港、新加坡、台灣、馬來西亞、菲律賓）

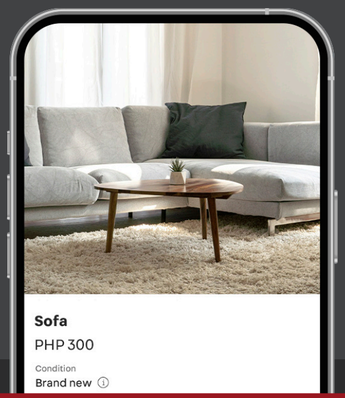
騙子偽裝成正當賣家，並提供極具吸引力的優惠。

按金及預購（香港、新加坡、台灣）

騙徒會刊登熱門或限量商品，並要求買家預先支付訂金或全額款項。

常見於：
Pokémon 卡、K-pop 周邊產品、活動門票、玩具及遊戲、音響產品





虛假陳述及未發貨（馬來西亞、菲律賓）

騙徒以不合理的低價出售潮流或優質商品，並表現得友善以博取買家信任。

常見於：
男裝及女裝、傢俬及家居

受害人付款後會面臨

- 運送一再拖延，騙徒找藉口推遲
- 無物流追蹤編號或提供虛假送貨更新
- 收到的商品有瑕疵或與刊登內容不符
- 賣家失聯或封鎖買家

人工智能生成圖像（僅作示意用途）

以下為 2025 年常見的詐騙類型：

2 平台外詐騙（香港、新加坡、馬來西亞）

騙子經常冒充買家，引導受害人前往偽冒網站以盜取款項。

釣魚連結（香港、新加坡、馬來西亞）

騙徒可能會索取用戶的電郵地址，並發送虛假的「付款確認」連結。

釣魚訊息（香港、馬來西亞）

騙徒可能會透過圖片或模糊化文字來規避偵測，並建議將對話移至 WhatsApp 或 LINE。

假冒電郵（新加坡）

騙徒會根據 Carousell 用戶名猜測電郵地址，並發送引用真實商品標題的電郵，令訊息看似正規可信。

受害人交涉後會面臨

- 不知情下洩露個人資料
- 被誘騙輸入登入資料
- 確認虛假付款請求
- 在偽冒網站進行交易

以上例子僅供說明用途。如有與任何真實人士、用戶名、機構或情況相似，純屬巧合，並非旨在描繪真實事件。

以下為 2025 年常見的詐騙類型：

3 數碼產品及遊戲詐騙（香港、新加坡）

數碼資產交易難以撤銷，因此常成為騙徒目標。

常見於：
遊戲禮品卡、遊戲虛寶、遊戲帳號

受害人付款後會面臨

- 收到無效、已用或錯誤地區的兌換碼
- 賣家託詞「系統延遲」，其後失聯
- 賣家未提供帳號登入資料便消失

人工智能生成圖像（僅作示意用途）

部分市場特有的詐騙手法：

菲律賓：「墊錢」詐騙

1 騙徒聲稱代他人購物，並要求賣家加價，差額作為佣金。

2 騙徒安排配送，並要求送貨員先行「墊錢」。在貨件送達前，騙徒已急於收取所謂「佣金」。

3 其後送貨員因地址無效無法送達，折返並要求退回墊付款項。

4 騙徒隨即失聯。

賣家損失了向騙徒支付的 PHP 1,000「佣金」，且必須向司機退還 PHP 6,000 的墊付款項。

台灣：退款詐騙

1 騙徒寄出有瑕疵的電子產品或與描述不符的商品。

2 他們向買家承諾退款，但以各種藉口不斷拖延，最終失聯。

Carousell 的防騙策略

我們採取全方位的信任與安全策略，以盡早偵測詐騙企圖、降低用戶風險，並在發現可疑活動時迅速採取行動。

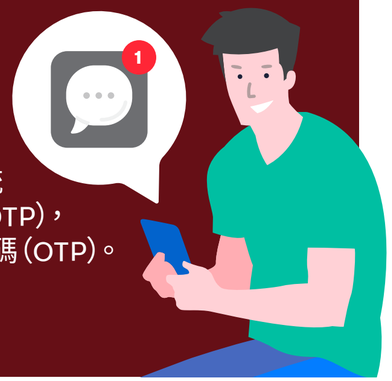
基於 AI 及機器學習的偵測與防護系統 1

我們運用人工智能 (AI)、
機器學習及數據科學技術，在每日數以百萬計的互動中偵測可疑行為。

步驟 1	步驟 2	步驟 3	步驟 4	步驟 5
收集	**過濾**	**分析**	**預防**	**人工審核**
AI 系統會掃描數以百萬計的商品刊登、聊天訊息及帳號活動。	數據會透過機器學習模型進行處理，該模型以過往詐騙模式訓練而成	機器學習模型識別可疑活動或異常模式。	高風險內容、商品刊登或帳號將被系統自動限制。	在需要時，審核人員會進一步對相關個案進行調查，並持續優化系統。

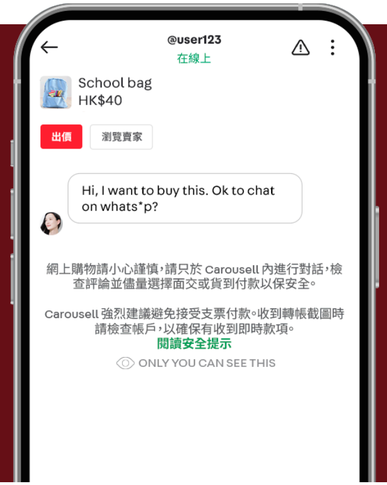
帳號安全與身份保護 2

我們持續強化身份驗證及登入安全，以降低假冒身份及帳號盜用的風險。在高風險登入情況下，系統會觸發短訊驗證碼 (SMS OTP)，而非僅依賴電郵一次性密碼 (OTP)。



更安全的交易方式 3

作為以 C2C (用戶對用戶) 交易為主的平台，用戶通常自行處理付款及送遞，過程中或存在風險。因此，我們持續設計以信任為核心的交易模式*，專門配合不同分類及市場用戶面對的獨特情況而設，例如透過**「購買」**按鈕提供的平台付款功能和合作快遞服務、透過**Carousell 認證**提供已驗證商品以及**首選商戶**計劃等。

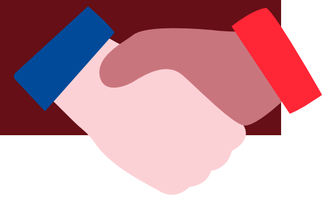


用戶教育與用戶社群舉報機制 4

我們會根據活動風險等級，在商品刊登頁面及對話視窗內主動顯示警示。用戶亦可透過每月的防騙教育活動，緊貼最新騙案趨勢。我們的用戶亦可舉報可疑活動以供調查，作為額外防線。

與政府部門合作 5

我們積極與各地執法部門及可信機構合作，分享詐騙趨勢，支援更廣泛的防詐騙工作。這些合作有助我們在平台內外同時強化偵測機制，完善安全措施。



* 相關計劃因地區而異。

圖片說明：即時聊天提示範例，提醒用戶切勿分享個人資料或在平台外交易。

用戶可採取的**防騙措施**

我們持續優化系統以防範詐騙，但最有效的保障始終來自用戶的警覺。以下是一些實用建議，幫助你提升安全意識：

請將所有對話留在 Carousell 平台內

避免轉至 WhatsApp 及 LINE 等通訊軟件繼續對話。**若對方堅持離開平台進行交易，應視為警號。**

注意電商詐騙常見特徵

「超抵價」、「限時優惠」、要求預付訂金或催促決定等，都是常見的騙案特徵。**不要急於作出決定，可先核實產品資料或向可信朋友查詢，再進行交易。**

切勿透露個人或付款資料

騙徒可能會**假借付款或送貨**為由，要求你提供電郵、手機號碼，甚至銀行應用程式的驗證碼。**請在個人檔案頁的「購買」或「銷售」中查看訂單詳情，確認是否真有交易。**

善用平台內安全功能

如平台提供付款功能，**建議使用平台付款功能和合作快遞服務。**這樣可以追蹤運送狀態，亦確保在確認收貨前，款項不會轉交賣家。如果平台的付款功能不適用於你的交易，請安排在安全的公共場所面交，以在付款前親自檢驗產品。

提防假連結與偽冒電郵

釣魚詐騙常以冒充 Carousell 的訊息或電郵作開端。

即使連結或電郵地址中含有「Carousell」詞，亦不代表一定是真實的。請務必仔細檢查完整的網站連結或寄件人電郵地址。

發現可疑情況，請立即舉報

不論是對話、產品還是連結，倘若你思疑已成為騙案的受害者請儘快透過平台舉報。你的舉報有助防止其他用戶受害。舉報是匿名進行，請放心使用。

carousell | 旋轉拍賣

support.carousell.com

以上例子僅供說明用途。如有與任何真實人士、用戶名、機構或情況相似，純屬巧合，並非旨在描繪真實事件。