carousell | 旋轉拍賣

2024 年地區詐騙趨勢報告

Carousell 如何打擊在香港、台灣及東南亞的詐騙行為

內容

前言

保護用戶、打擊詐騙、建立信任

網絡詐騙不只是影響平台，更是直接影響每一位用戶的安全和信任。本報告綜合了 Carousell 於 2024 年在香港、馬來西亞、菲律賓、新加坡及台灣觀察到的主要詐騙手法，並說明我們如何透過更智能的科技、即時警示，以及與各地合作夥伴的協作，主動應對詐騙問題。

主要發現

最常見的詐騙手法

釣魚詐騙（假冒買家、冒充客服）、電商詐騙、假貨買賣、演唱會及活動門票詐騙。

騙徒的操作手法

騙徒常以緊迫感、冒充身份，或引導用戶轉至 Carousell 以外的平台對話進行詐騙，更加仿傚 Carousell 的真實功能以增加可信度。

Carousell 的反詐騙行動

於 2024 年，我們大規模採取以下措施，預防詐騙並保障社群安全：

- **限制了 1.28 萬條** 可疑連結
- **封鎖了 42.2 萬個** 可疑帳號
- **攔截了 72.7 萬個** 電郵地址
- **調查了 30.9 萬宗** 社群舉報

報告編製單位 Carousell 防騙及交易安全工作小組（2025 年 7 月）

為什麼詐騙持續發生？
Carousell 又如何應對？

*具備買家保障的平台付款功能現時適用於香港、馬來西亞及新加坡；Carousell 認證計劃則僅於新加坡及馬來西亞的部分產品分類提供。

“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。騙徒比以往更能迅速適應用戶行為與平台的防護措施。他們會仿冒平台功能、透過多個渠道操作，甚至利用人工智能 (AI) 製作出高度擬真的詐騙情境。

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 每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. 更安全的交易方式，例如具備買家保障的平台付款功能，以及 Carousell 認證計劃 (Carousell Certified)*

   購買 買家保障
3. 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。當用戶忽視內置警告，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。

我們發佈這份報告，是希望幫助你了解詐騙的運作模式、學懂如何辨識風險，以及認識 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

各地常見詐騙手法

雖然不同市場的詐騙看起來可能有所差異，但其實手法大致相同：目的是引誘用戶轉帳或提供個人資料，往往涉及將對話引導到 Carousell 平台以外。以下是我們於 2024 年在區內觀察到最常見的幾種詐騙類型：

1

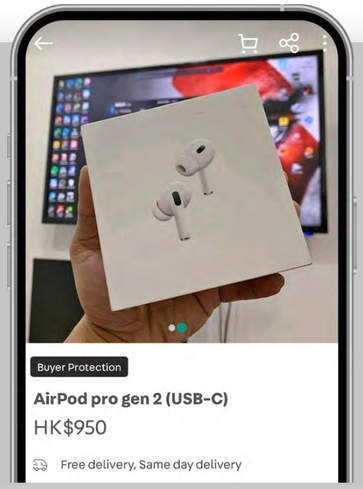
假貨詐騙

最常見於香港及新加坡，主要涉及售賣假冒波鞋及名牌時尚產品。

2

電商詐騙

騙徒針對熱門電子產品，利用用戶急於搶購或尋找優惠的心理行騙，收款後便立即消失。產品往往配以非常逼真的圖片，令人難分真假。



圖片說明: 虛假 AirPods 詐騙的產品圖片範例

3

演唱會及活動門票詐騙

在香港及新加坡尤其常見。騙徒會聲稱手上有熱門或已售罄活動的門票，並以低價出售。付款後不是沒有寄出門票，就是寄出假票。

4

假買家詐騙(釣魚詐騙類型)

騙徒會冒充有意購買的買家，要求賣家提供電郵地址，聲稱用作付款或送貨用途。之後受害人會收到模仿 Carousell、銀行或物流公司的假網站連結，引導他們輸入個人或銀行資料。騙徒有時會提及 Carousell 的真實功能 (例如買家保障)，以增加可信度。

圖片說明: 騙徒會發送假冒 Carousell 的付款確認或訊息，誘騙賣家提供資料。

5

假冒 Carousell 客服(釣魚詐騙類型)

主要分為兩種手法:

1. 騙徒假扮買家，聲稱出現系統錯誤，並提供假的客服聯絡方式。一旦聯絡上所謂的客服，對方便會誘使用戶透露個人或銀行資料。
2. 騙徒直接假冒 Carousell 客服，以 CarouDM、電郵或 SMS 發送釣魚連結。

圖片說明: 內容透過虛假的「結帳失敗」及安全漏洞警示，誘騙用戶掃描二維碼，從而進入惡意網站，以盜取資料。

各市場最常見的詐騙類型

馬來西亞: 時尚產品詐騙（賣家失聯）

Green polo
RM55

香港: 演唱會門票詐騙

演唱會門票
(賣家失聯，寄出假券)
HK$1,099

台灣: 限時五折優惠詐騙

50% off 休閒卡其褲裙
NT$150

Singapore: Enabler 詐騙（兼職工作、電子產品、物業相關）

售盤
S$300,000

菲律賓: 數碼相機詐騙

CCD 相機
(賣家失聯)
PHP 5,999

部分市場特有的新型詐騙手法

菲律賓：代購/貨到付款「墊錢」詐騙

新加坡: Enabler 詐騙

○ 詐騙個案示例: 釣魚詐騙如何一步步發生

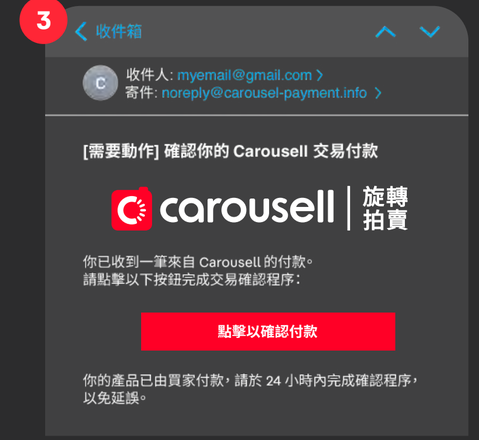
1

Ana 剛在 Carousell 刊登她的相機，就收到一則來自買家的訊息。

2

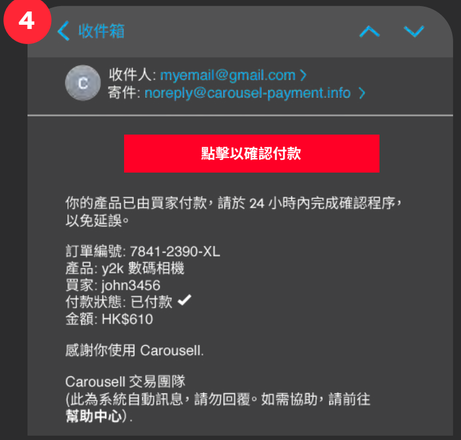
對方語氣禮貌，看起來很誠懇。為了儘快成交，Ana 還是回覆了，並故意將電郵地址拆開以避開系統偵測。

3



不久後，她又收到對方訊息。那封電郵看起來極像來自 Carousell 的。Ana 點了那個按鈕。

4



該電郵看起來與 Carousell 幾乎一模一樣，畫面要求她輸入銀行資料及手機接收到的 6 位數字的驗證碼「以作核實」。

5

她照做了，以為這樣就能收到款項。但是幾分鐘後，Ana 發現自己銀行帳戶的資金被轉走了。

以下故事為了說明用途，靈感取自真實個案。

個案分析: 究竟發生了什麼事?

Ana 成為了釣魚詐騙的受害者。騙徒先要求電郵，再發送假冒 Carousell 的訊息和網站，引導她輸入個人資料。

當她輸入銀行帳戶資料及驗證碼後，詐騙集團便成功取得登入憑證，直接從她的帳戶中盜走款項。

如何保護自己?

- 切勿分享電郵、手機號碼或通訊軟件帳號
- 不要透過 Carousell 平台以外的連結確認付款
- 仔細檢查網址，避免點擊可疑結尾的連結: carousell-payment.info、carousell-verification.com
- Carousell 官方連結一律以以下網址結尾: carousell.com、carousell.sg、carousell.ph、carousell.app.link。由 Carousell 發出、有關你帳號資料的電郵，只會來自 @carousell.com 或 @thecarousell.com
- 注意應用程式內的安全提示，它們是為了保障你的安全而設計的

全面打擊詐騙：
Carousell 在 2024 年如何保障數百萬用戶的安全？

從源頭阻截高風險行為

已封鎖可疑連結：
1,280,000 條

已攔截可疑電郵地址：
727,000 個

已截停可疑二維碼：
20,000 個

為保障社群安全，當用戶分享連結、電郵及二維碼時，Carousell 會自動封鎖，從源頭減低發生詐騙的風險。

用戶嘗試分享手機號碼時，平台共發出 **2,300 萬次安全警示**

當中 **82% 用戶仍然選擇繼續分享**

由於不少面交交易確實需要通訊，Carousell 並沒有禁止分享手機號碼，但會透過彈出式警告明確提示風險，協助用戶在分享前三思。

對抗詐騙，需要平台與用戶共同努力

詐騙活動往往以「階段式」出現，騙徒會在一段時間內集中攻勢，直至平台防禦系統發揮效果，之後又以新手法捲土重來。

因此除了預防機制，迅速反應也十分重要。Carousell 與用戶社群同樣擔當關鍵角色，在發現新型詐騙時即時回應，以減低損害。

已封鎖可疑帳號：
422,000+

社群舉報總數：
309,000+

平台執法與用戶舉報相輔相成，才能在廣泛範圍內迅速反制詐騙，讓每位用戶每天都能更安心地使用平台。

以上數據為 Carousell 內部統計，涵蓋 2024 年 1 月至 12 月。

Carousell 的防詐騙策略

Carousell 採取多層面的信任與安全策略，結合科技、平台功能、用戶舉報及跨市場的合作。我們的目標是儘早識別詐騙行為、減低用戶風險，並在發現可疑活動時迅速作出反應。

交易安全大使: **安安**

基於 AI 及機器學習的偵測與防護系統

Carousell 自主研發了基於人工智能、機器學習及數據科學的系統，用於偵測產品、聊天及用戶活動中的可疑行為。這些技術幫助我們識別詐騙模式，封鎖有害內容，並且標記高風險行為。

*圖片說明：帳號被停權的範例，提醒用戶不要繼續交易。聊天室亦會被關閉，避免進一步聯絡。

更安全的交易方式

Carousell 是一個以 C2C（用戶對用戶）為主的交易平台，大部分交易在用戶之間直接完成，變數亦相對較多。

由於平台外的詐騙行為難以偵測，為減少風險，Carousell 提供多項功能，協助將交易儘量留在平台內，減少轉移至第三方渠道時的風險。

當中包括設有買家保障的平台付款功能和合作快遞服務，以及 Carousell 認證計劃（已認證的產品並提供送貨服務）*

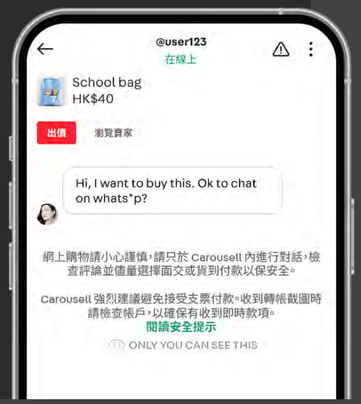
*平台付款功能台付款功能現時適用於香港、馬來西亞及新加坡；Carousell 認證計劃則僅於馬來西亞及新加坡提供。

用戶教育與社群舉報機制

Carousell 每月都會透過平台、幫助中心及電郵，向用戶推廣防詐騙資訊及最新騙案趨勢。

平台會在聊天室內發出即時警示，提醒用戶避免分享個人資料。若對方帳號已被停權，系統亦會在聊天室內顯示警告橫額，提醒用戶在進行交易前須多加注意。

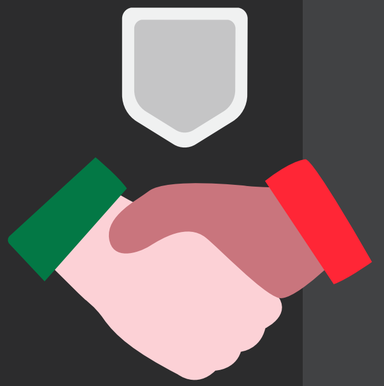
*圖片說明：即時聊天提示範例，提醒用戶切勿分享個人資料或在平台外交易。



與政府部門合作

Carousell 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。



用戶可採取的防騙措施

Carousell 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

騙徒經常要求轉至 WhatsApp 及 Telegram 等通訊軟件繼續對話，避開平台的安全偵測機制。若對方堅持離開平台進行交易，應視為警號。

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。

注意電商詐騙常見特徵

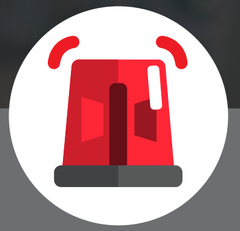
「超抵價」、「限時優惠」、要求預付訂金或催促決定等，都是常見的騙案特徵。不要急於作出決定，可先核實產品資料或向可信朋友查詢，再進行交易。

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。

善用平台內安全功能

如平台提供付款功能，建議使用內建方式付款及安排送貨。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。



發現可疑情況，請立即舉報

不論是對話、產品還是連結，只要感覺不對勁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

提供的例子僅供說明之用。所有與真實人物、用戶名稱、實體或情況的相似或引用均純屬巧合，並非有意為之，亦不代表任何實際事件。