

認識

善用數碼工具及網絡陷阱

香港警務處
網絡安全及科技罪案調查科
陳穎 高級督察



香港的科技罪案數字

2024 Q1 – Q3

CASE #

25,118

LOSS \$. (MIL)

3,887



香港的科技罪案數字

2025 Q1 – Q3

CASE #

3%

24,370

LOSS \$. (MIL)

18.1%

4590



最多 VS 最貴

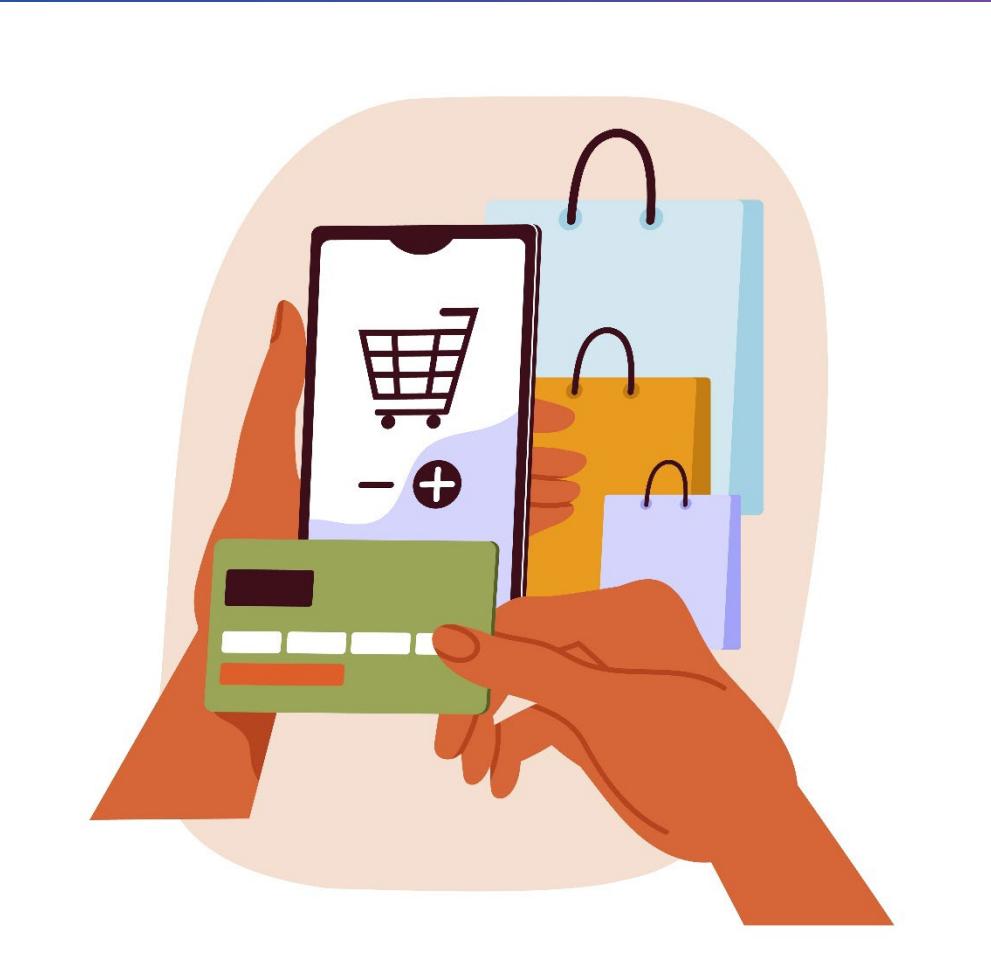


1	網上購物騙案	9,569 宗 (39%)
2	投資騙案	3,709 宗 (15%)
3	求職騙案	3,566 宗 (15%)



1	投資騙案	HK \$2,4131M (52.6%)
2	求職騙案	HK \$772M (16.8%)
3	網上情緣騙案	HK \$373.3M (8.1%)

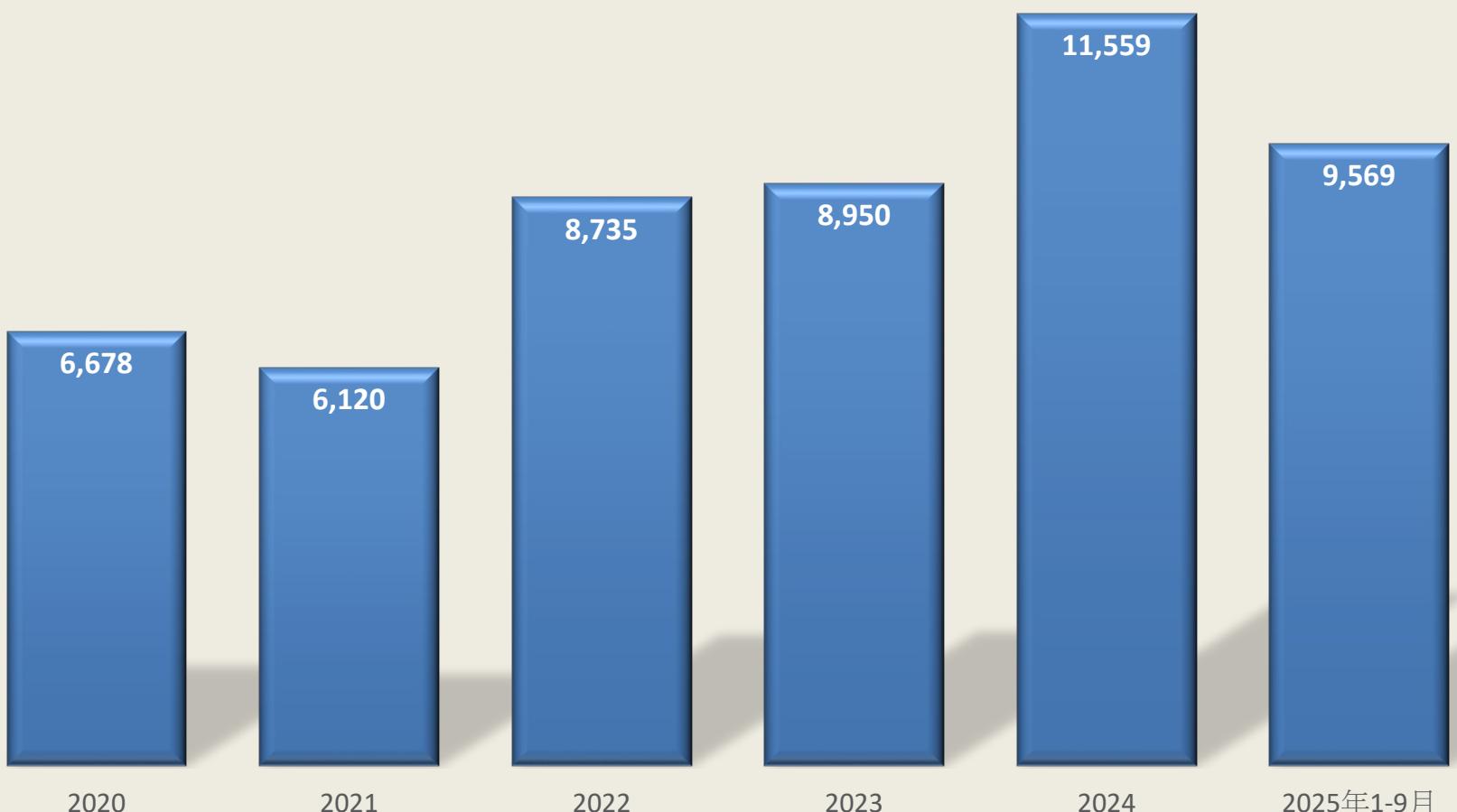
網上購物騙案



網上購物騙案(過去5年)

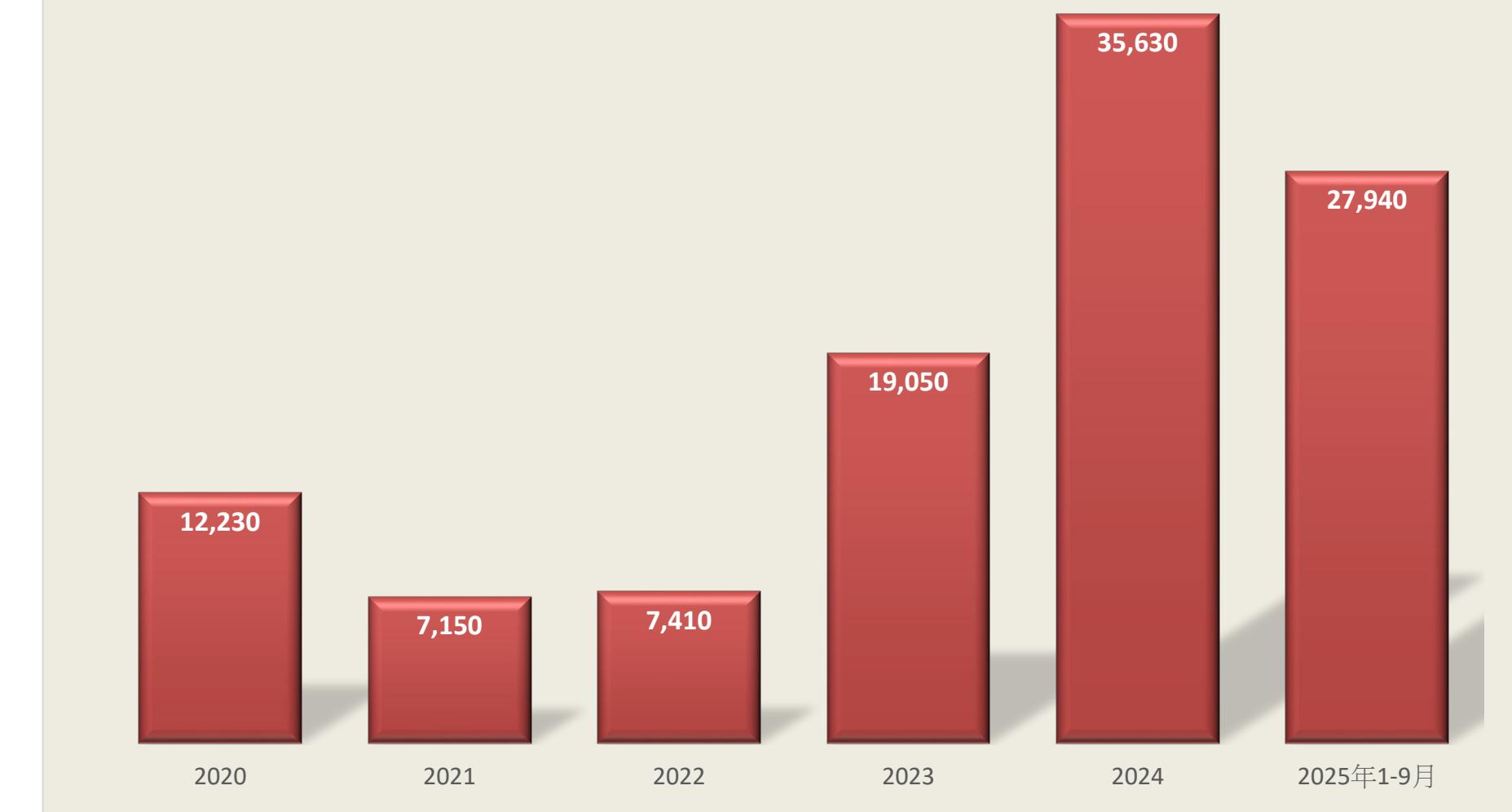
案件宗數

■ 案件宗數



損失金額(萬)

■ 損失金額(萬)

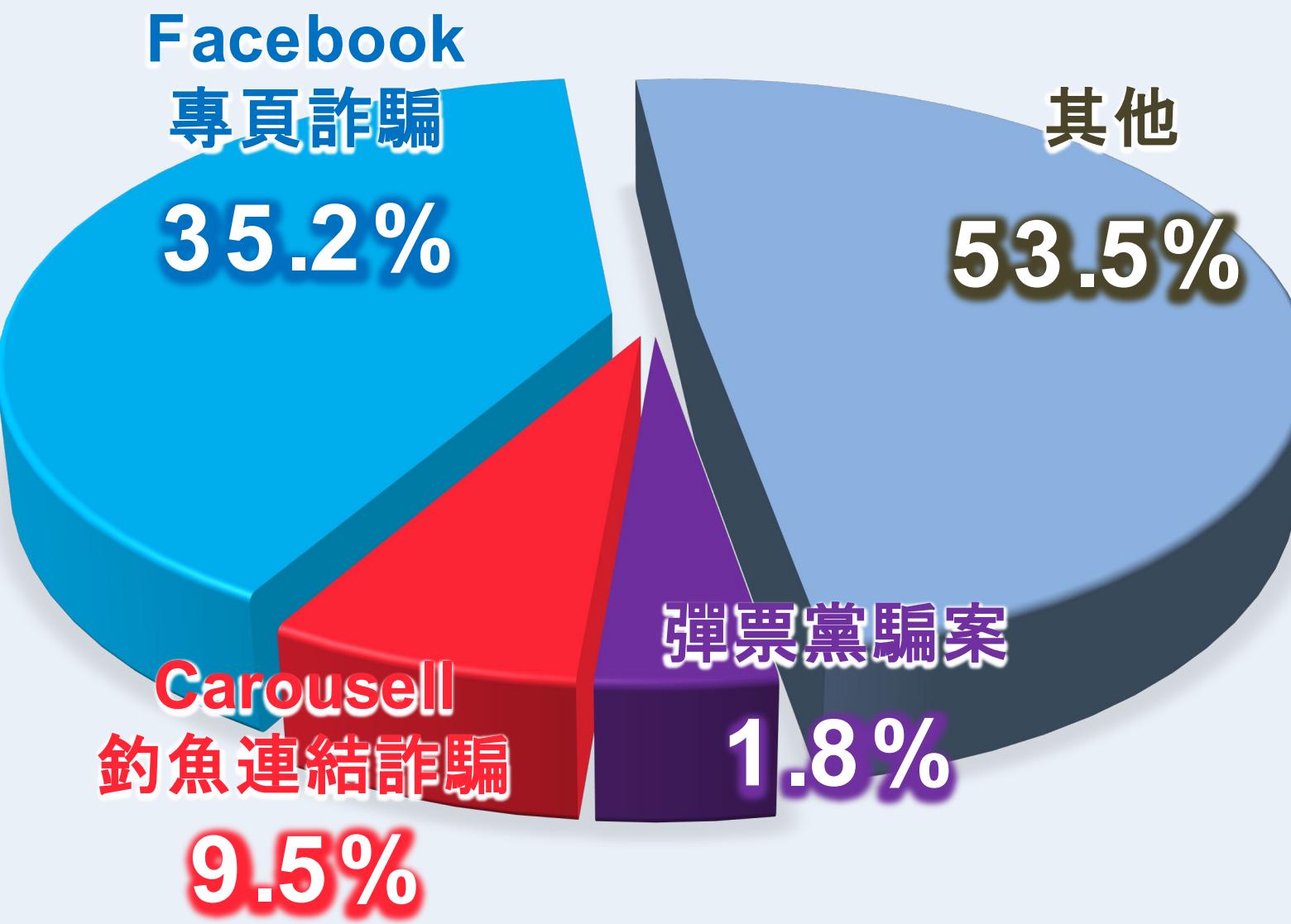


三種常見的網上購物騙案犯案手法

2025年1-6月年網上購物騙案的損失金額



2025年1-6月網上購物騙案的犯案手法



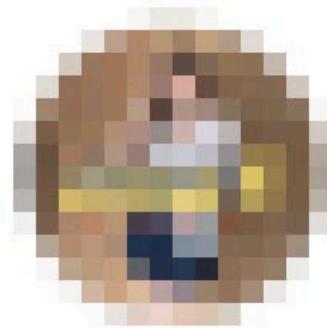
Facebook網購專頁騙案

This screenshot shows a Facebook page profile for a shopping website. The profile picture features a person's face next to a yellow smartphone displaying a product page. The page name ends in 'HK'. Below the profile picture, it says '13 萬讚好次數 · 15 萬位追蹤者' (130,000 likes · 150,000 followers). The top navigation bar includes 'WhatsApp', '讚好', and '搜尋' buttons. The main content area has tabs for '帖子' (Posts), '關於' (About), 'Mentions', 'Reels', '相片' (Photos), '影片' (Videos), and '更多' (More). The '帖子' tab is selected. The '简介' (About) section contains a warning message about counterfeits and scam attempts. The '精選' (Selected Posts) section shows two posts from other users, one from '1月8日' (January 8th) and another from '5天前' (5 days ago).

This screenshot shows another Facebook page profile for a shopping website. The profile picture is a small circular image. The page name ends in 'HK'. Below the profile picture, it says '508 讚好次數 · 2,148 位追蹤者' (508 likes · 2,148 followers). The top navigation bar includes '讚好' and '搜尋' buttons. The main content area has tabs for '帖子' (Posts), '關於' (About), 'Mentions', '評論' (Comments), '追蹤者' (Followers), '相片' (Photos), and '更多' (More). The '帖子' tab is selected. The '简介' (About) section lists the page's business type as '專頁 · 購物服務 · 百貨公司' (Business Page · Shopping Services · Department Store Company). It also provides the address '葵涌葵豐街 Profit Industrial Building, Hong Kong, Hong Kong, Hong Kong, Hong Kong', the URL 'facebook.com/profile.php?id=61574531753477', and operating hours '24 小時營業' (24-hour service). The '帖子' section displays a post from a user sharing information about a product, including a large red circle with the word '假' (Fake) overlaid.

Facebook網購專頁騙案

專頁

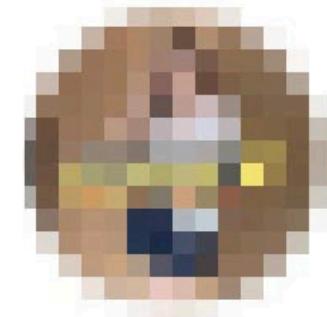


[REDACTED] HK

購物與零售 · 5.8 km · 營業中 · 15 萬位粉絲 ·
過去 2 星期內有超過 10 篇帖子

[REDACTED] HK 專業團隊搜羅全球至抵名牌筍貨
⭐十年信譽口碑 🤝 正貨信心保證 ⭐ ❤️ 中歐美加……

追蹤



[REDACTED] HK

購物服務 · 6 km · 24 小時營業 · 2,148 位粉
絲

追蹤

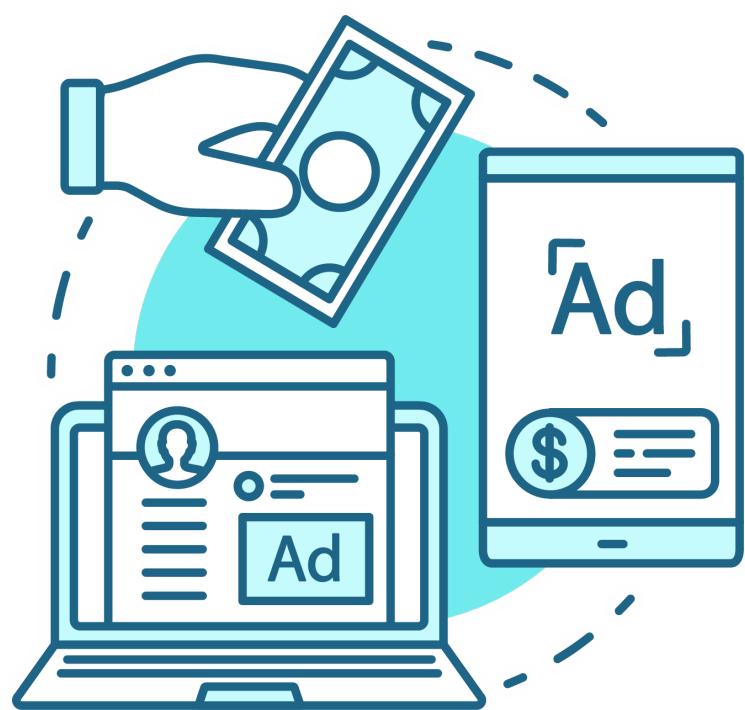
假

Facebook虛假專頁騙案的特徵

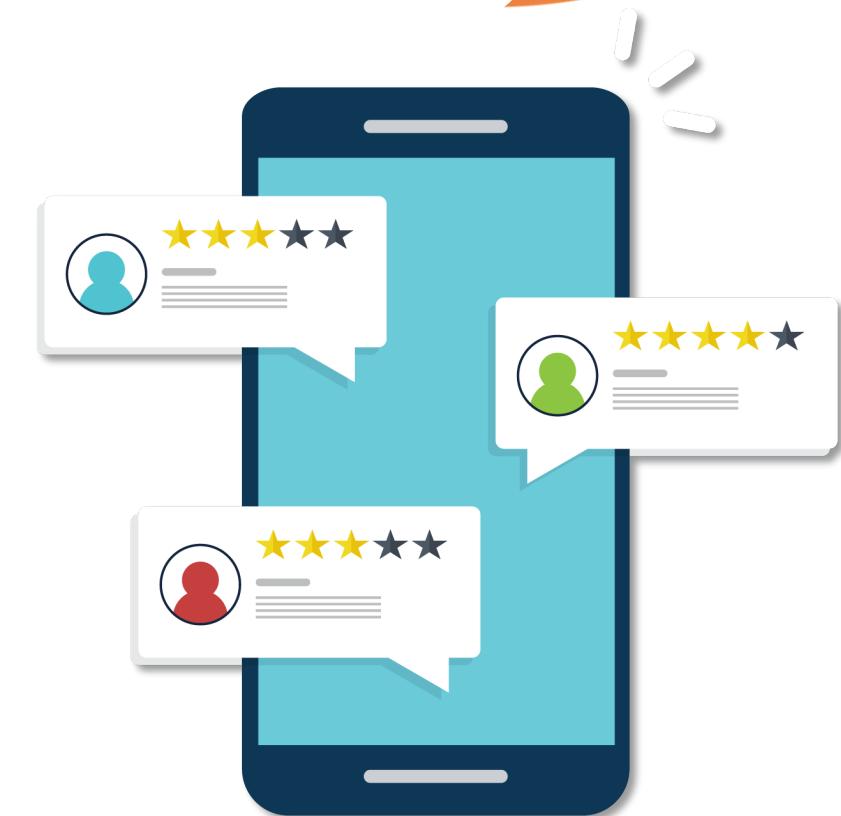
1



2



3



騙徒開設的專頁一般只經營很短的時間，例如數天或數星期，而且沒有實體店地址或辦公室電話

管理人員來自不同國家及刊登廣告以提升知名度

會聘用打手給予好評或留言，製造多人光顧假象



Carousell釣魚連結騙案

1

假扮買家
並向賣家提出以「**平台收款功能**」交易並要求索取
賣家的**電郵地址**

2



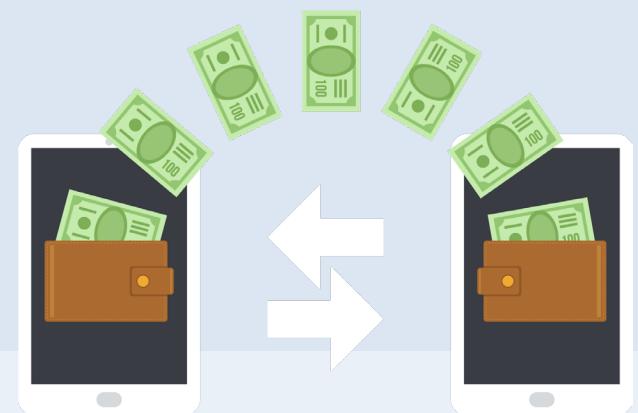
賣家收到**假冒 Carousell 的電郵**，並
要求按下超連結以收
貨款

3



進入虛假網站
輸入網上銀行帳戶
登入資料及**一次性密碼**
以收取貨款

4



當騙徒獲得有關資料後就
會將受害人的**資產轉移**

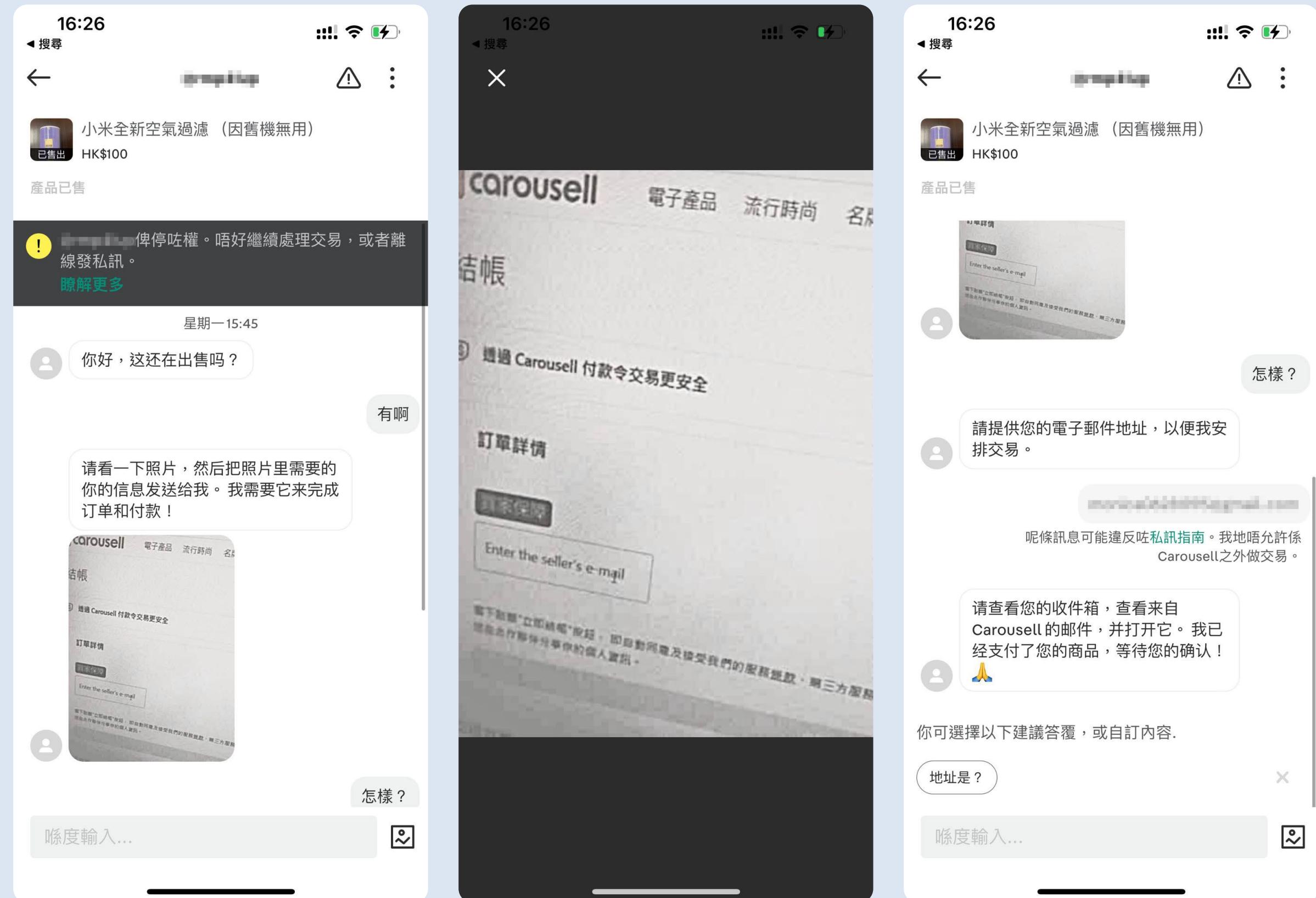
此類利用釣魚連結的 **carousell** 網購騙案

於2025年1-6月共錄得**624**宗，涉及損失超過**3,400萬**港元

Carousell釣魚連結騙案手法示範

1

假扮買家
並向賣家提出以「**平台收款功能**」交易並要求索取
賣家的**電郵地址**



Carousell釣魚連結騙案手法示範

2



carousell | Safe receipt of money

Stage 1/2
Receipt of funds

1. Ordering information
Information about the buyer.
– Buyer's full name*

– Address for delivery*

– Order number*

Stage 2/2: Get Money

小米全新空氣過濾 (因舊機無用) 100 HKD

Receipt of funds
The product is already paid for!
After receiving the money on your card send the goods to the buyer according to the specified data or by the courier who will contact you within 12 hours.

After we ship the item, please provide the buyer with the tracking number. Item must be shipped within 3 days of receipt of funds

Protection Carousell
✓ All your data is confidential and protected, after receiving the money you have to send the goods
✓ A dedicated team at your service

Total 100 HKD

Carousell釣魚連結騙案手法示範

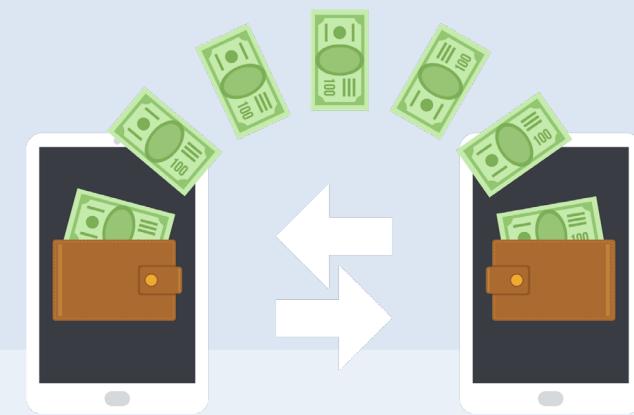
3



進入虛假網站
輸入網上銀行帳戶
登入資料及一次性密碼
以收取貨款

The top screenshot shows a Carousell payment page for 100 HKD, asking for advance payment. It lists several banks for FPS transfer, with 'Hang Seng Bank' selected. The bottom screenshot shows a login page for Hang Seng Personal Banking, prompting the user to log on using a new method. It includes fields for 'Enter your username' and 'Enter First Password', and a 'Continue' button.

4



當騙徒獲得有關資料後就
會將受害人的**資產轉移**

Carousell釣魚連結騙案防騙貼士

詐騙的手法

1

要求提供電郵地址以進行所謂的「付款流程」

2



在虛假的Carousell付款平台輸入自己的個人及帳戶資料



絕不需要用戶
提供電郵地址以進行付款

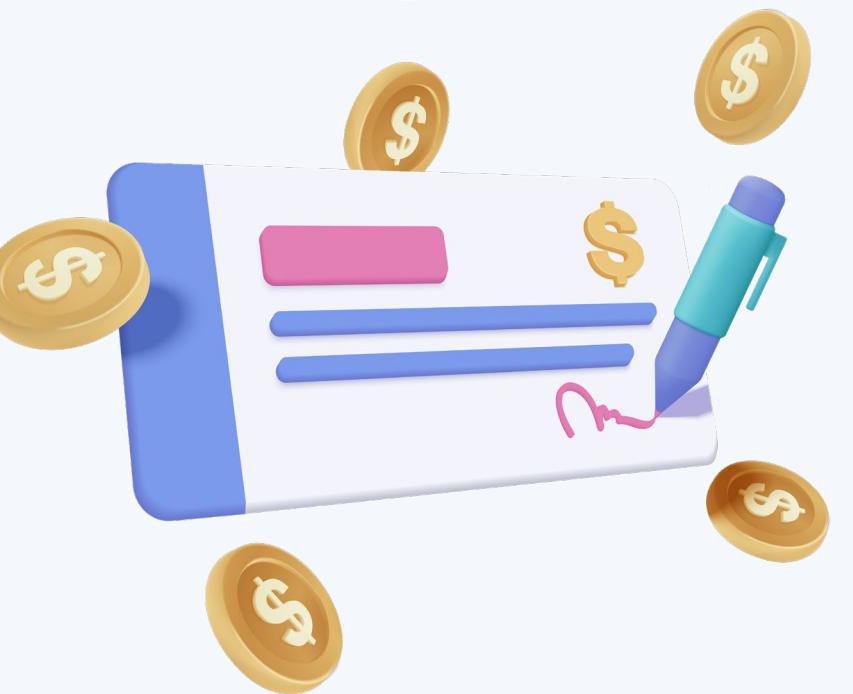
官方網址都以「carousell.com」或
「carousell.com.hk」結尾。

「彈票黨」騙案手法

1

提出以「支票付款」完成交易
並且願意親身面交以換取賣家信任

2



以空頭支票入數
讓賣家以為已經成功收款

提防「彈票黨」防騙貼士

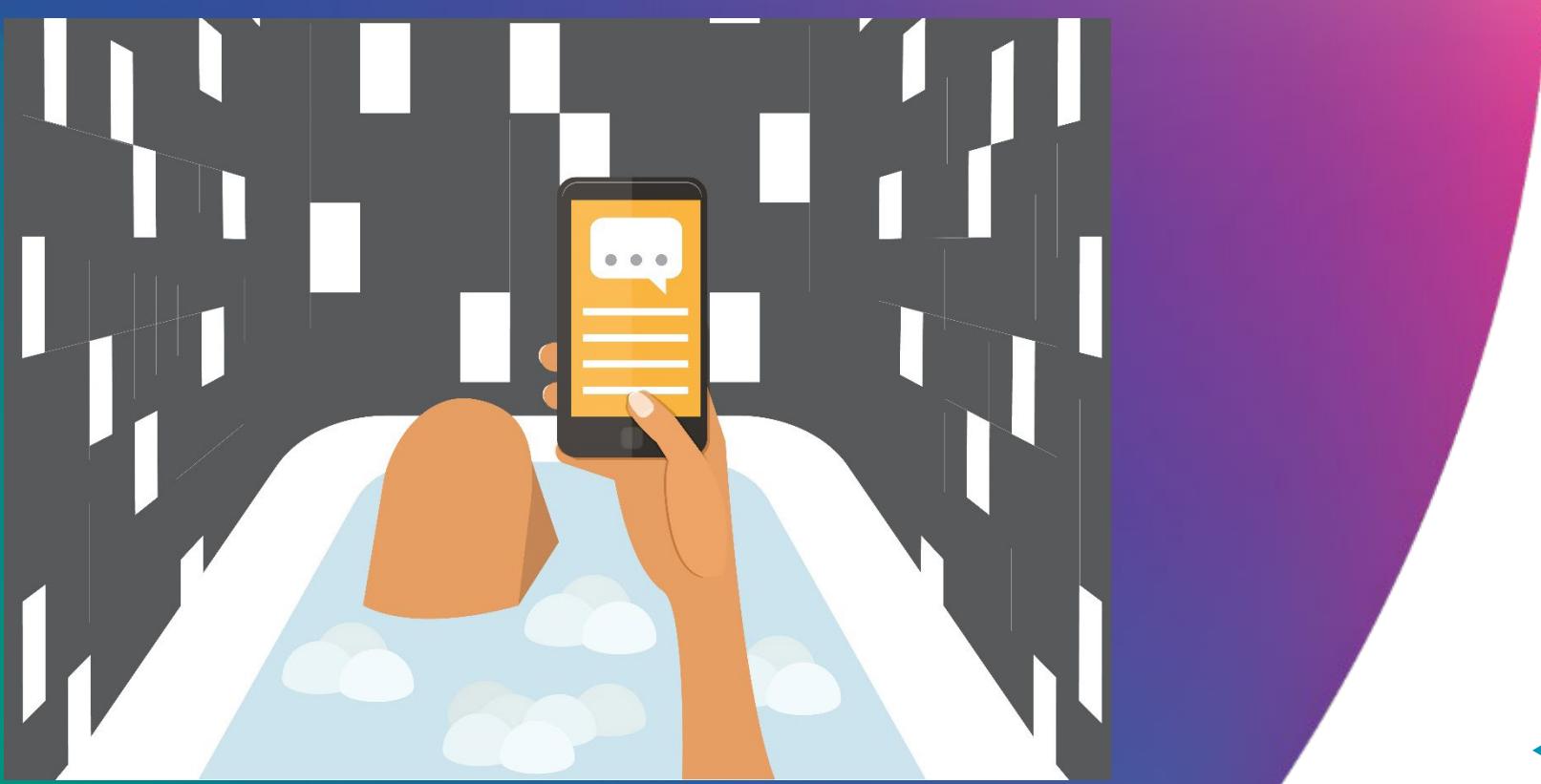


「賬面結餘」/「戶口結餘」

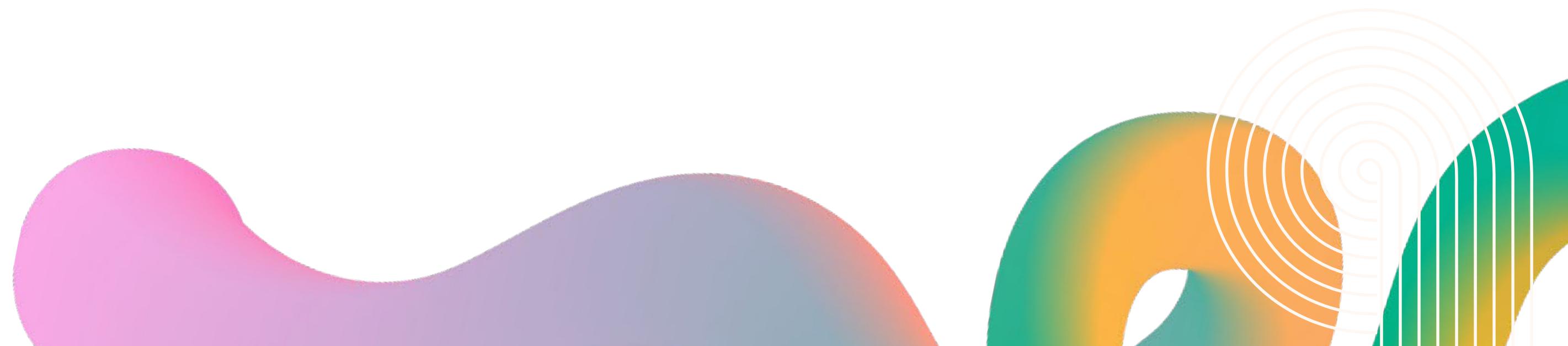


可用結餘



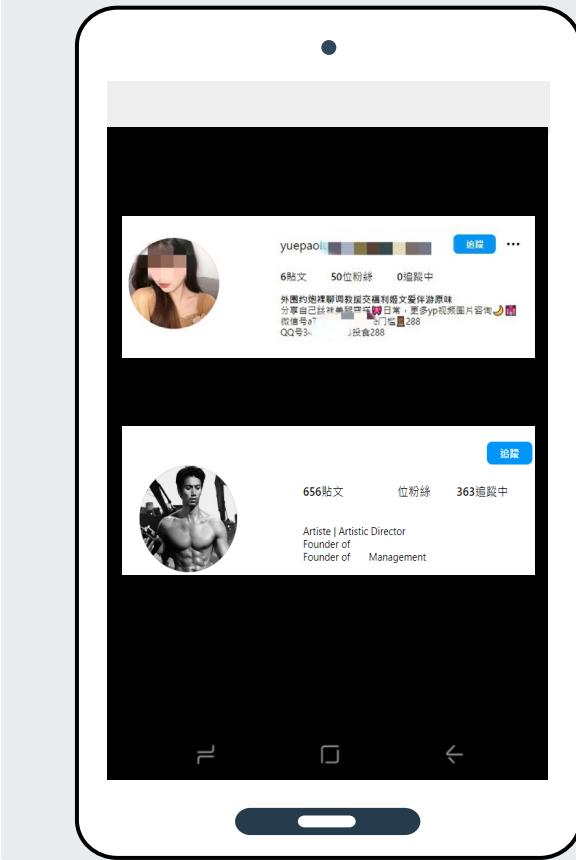


裸聊騙案



裸聊勒索手法

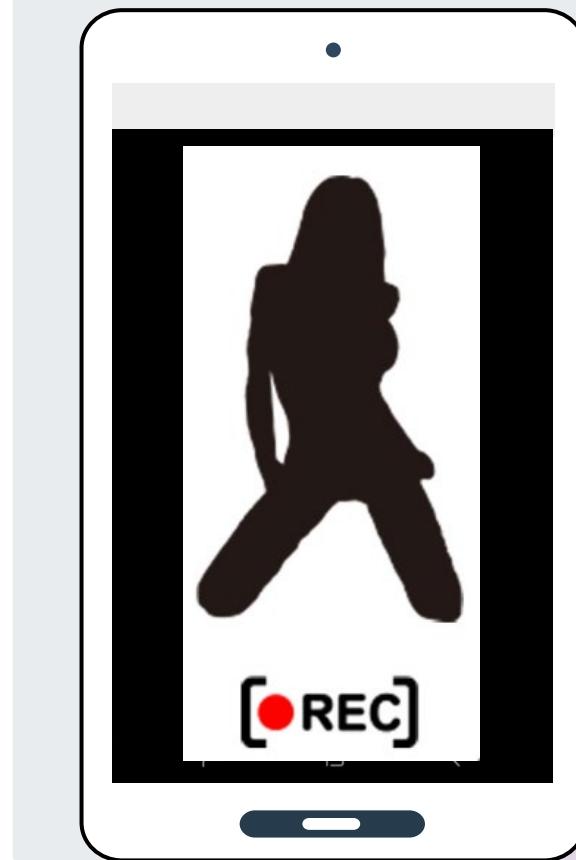
① 騞徒以美女或俊男頭像吸引網友



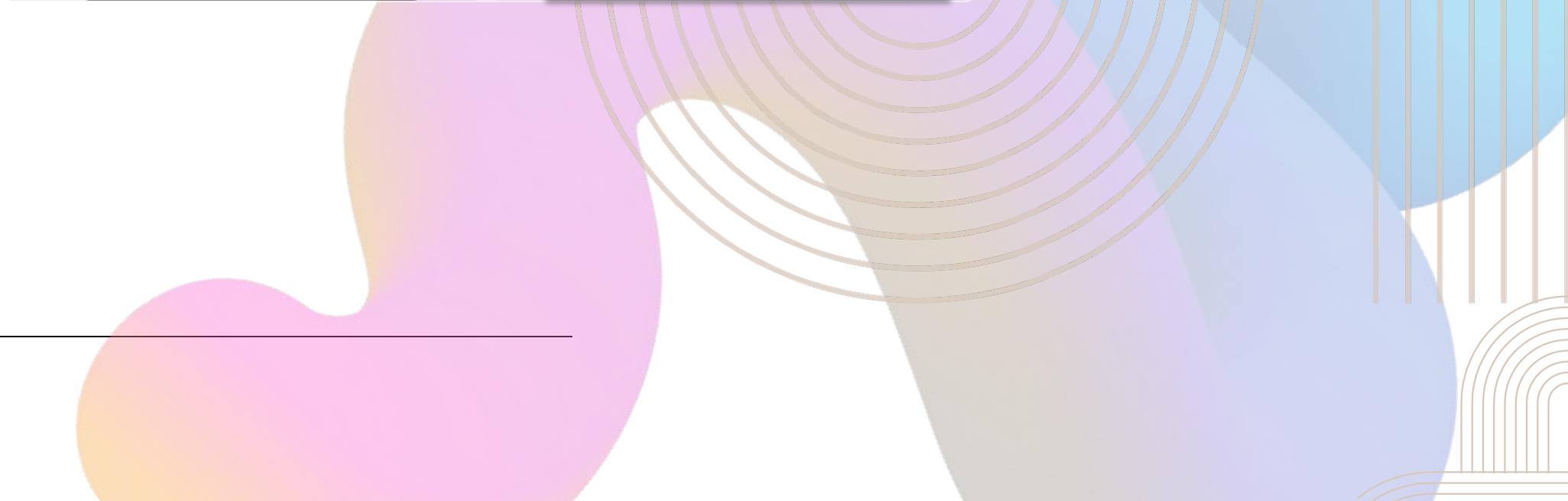
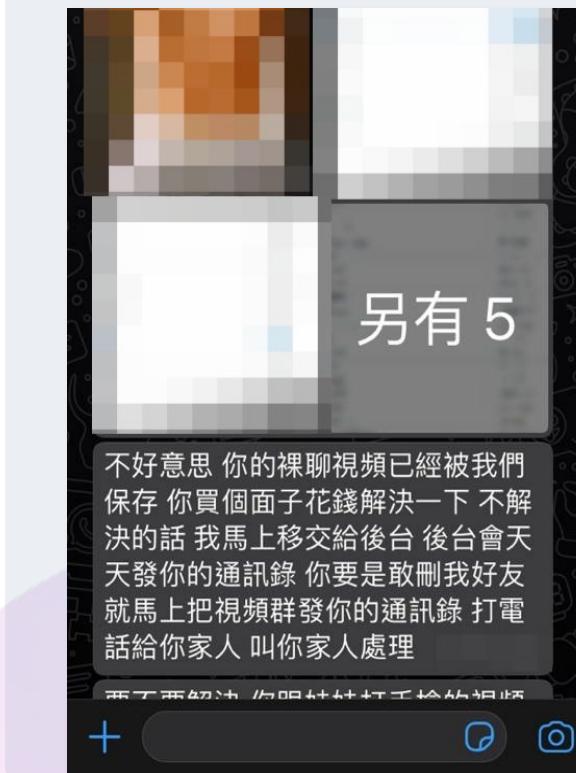
② 套取個人資料或誘使下載惡意程式以盜取通訊錄資料



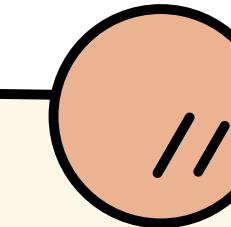
③ 引誘受害人進行裸聊並拍下不雅片段



④ 勒索受害人付款否則將裸聊片段轉發親友



裸聊勒索預防及處理

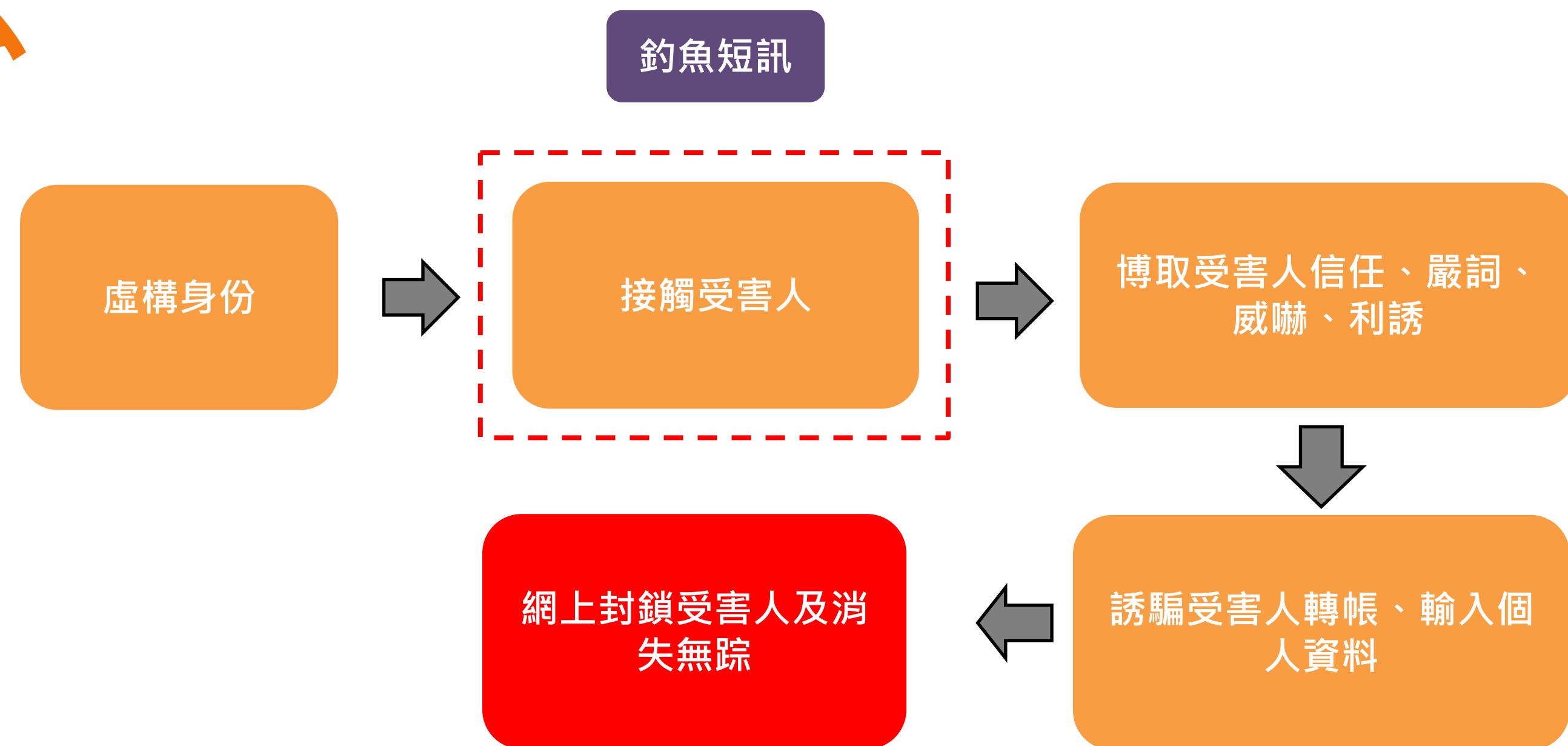


- 切勿在視像聊天期間裸露身體
- 切勿點擊不明來歷的超連結或下載可疑程式
- 切勿輕信對方是以真面目示人



釣魚(PHISHING): 詐騙的開端

騙徒常用 手法



短訊釣魚信息 (SMS Phishing)



短訊釣魚信息 (SMS Phishing)

網上求職騙案



網上投資騙案

為回饋新老用戶，特此建立線上交流群組，並且分享強勢上漲 20% 股票。安卓用戶需要回復“1”彈出客服名片添加領取相關福利和加入群組名額預約免費線上課程教學。蘋果用戶可直接添加名片。 07:38

網上情緣騙案



援交騙案



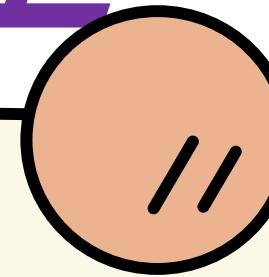
戶口盜用

WhatsApp 官方檢測您賬號
存在安全風險，12小時後將
永久註銷；為確保賬號安
全，請聯系客服完成驗證：
whsatapp-wh.com

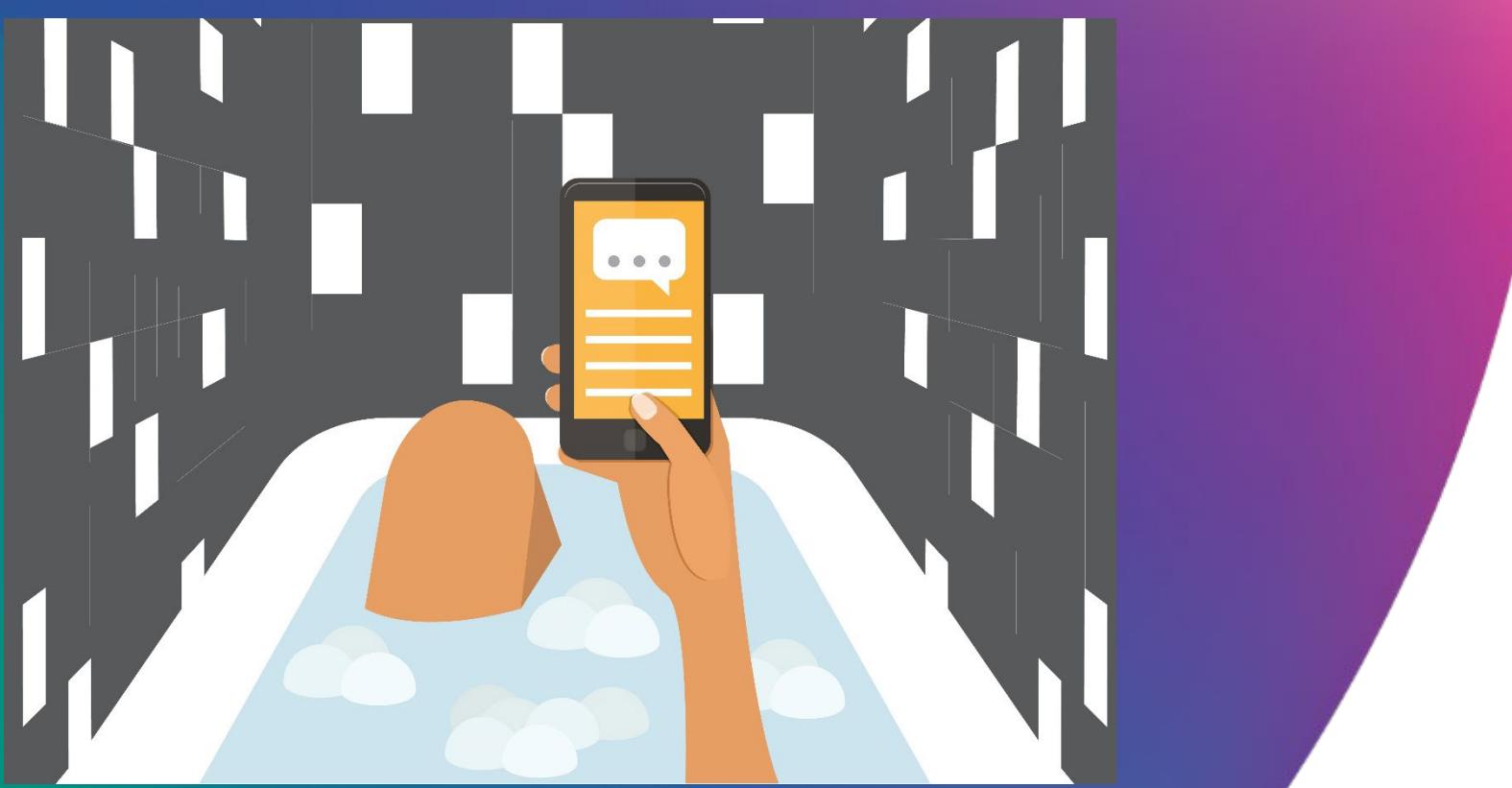
釣魚短訊

[易通行：自動繳費不成功] 你未能成
功透過指定儲值戶口於 18/08/2023 繳
付隧道費 HK\$55。
請透過易通行 <https://bit.ly/3EgNiGw>
繳費，並於 26/08/2023 前完成付款。

預防及處理



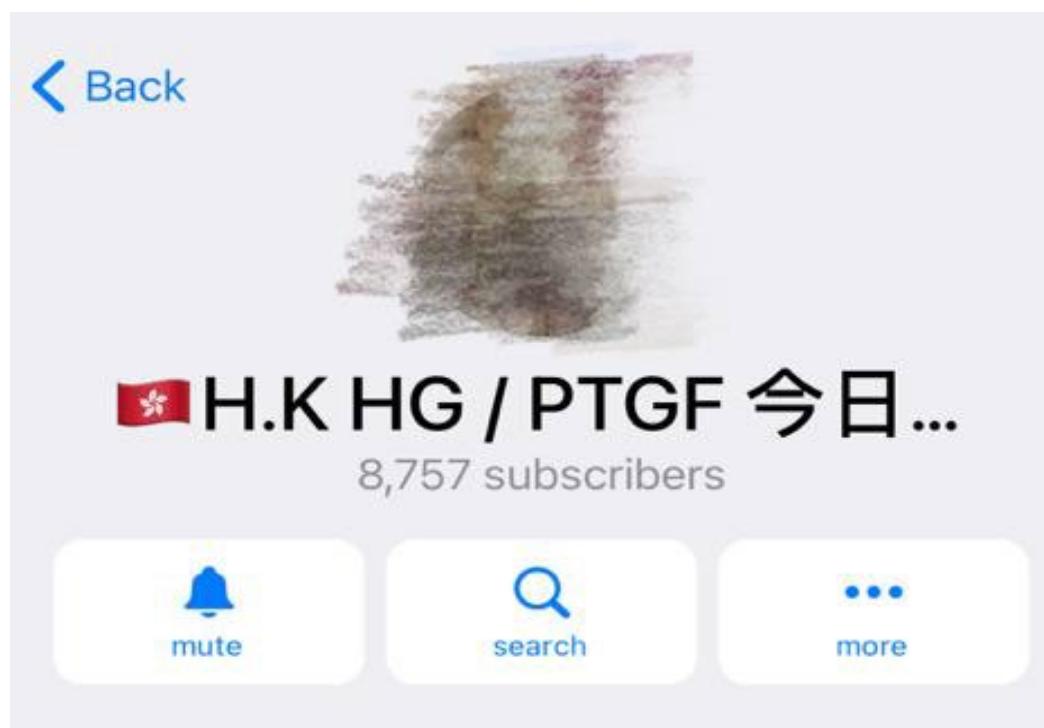
- 勿與陌生人視像通話，如遇裸露要求對話應立即終止；
- 勿透露個人資料、避免成為目標；
- 切勿點擊可疑連結或下載不明程式；
- 及
- 建立開放溝通，遇上問題時，可以放膽尋求父母協助。



網上援交騙案

援交騙案手法

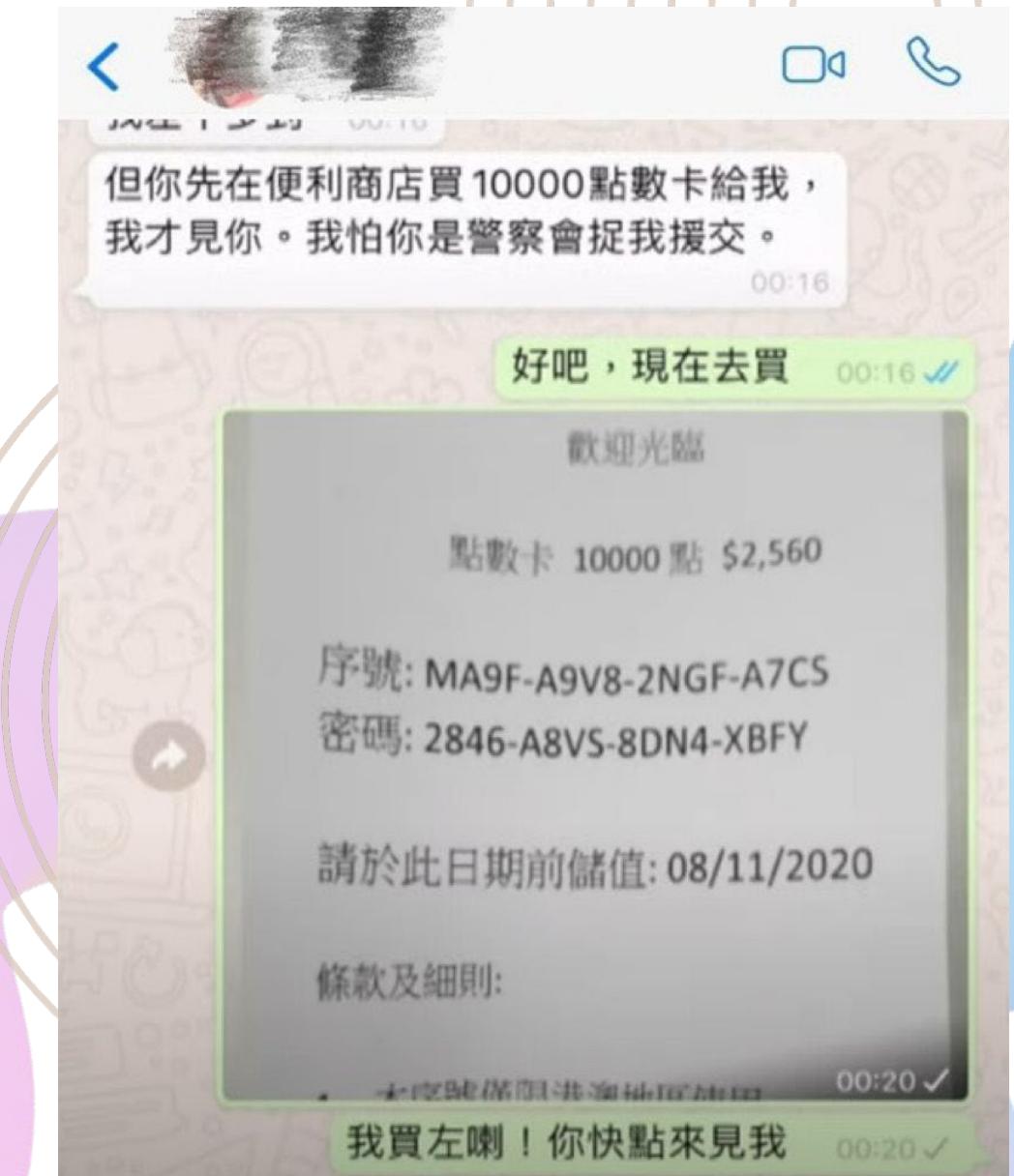
① 騙徒於社交媒体/通訊群組/約會軟件，聲稱提供援交或性服務



② 談論價錢、套取個人資料及邀約會面

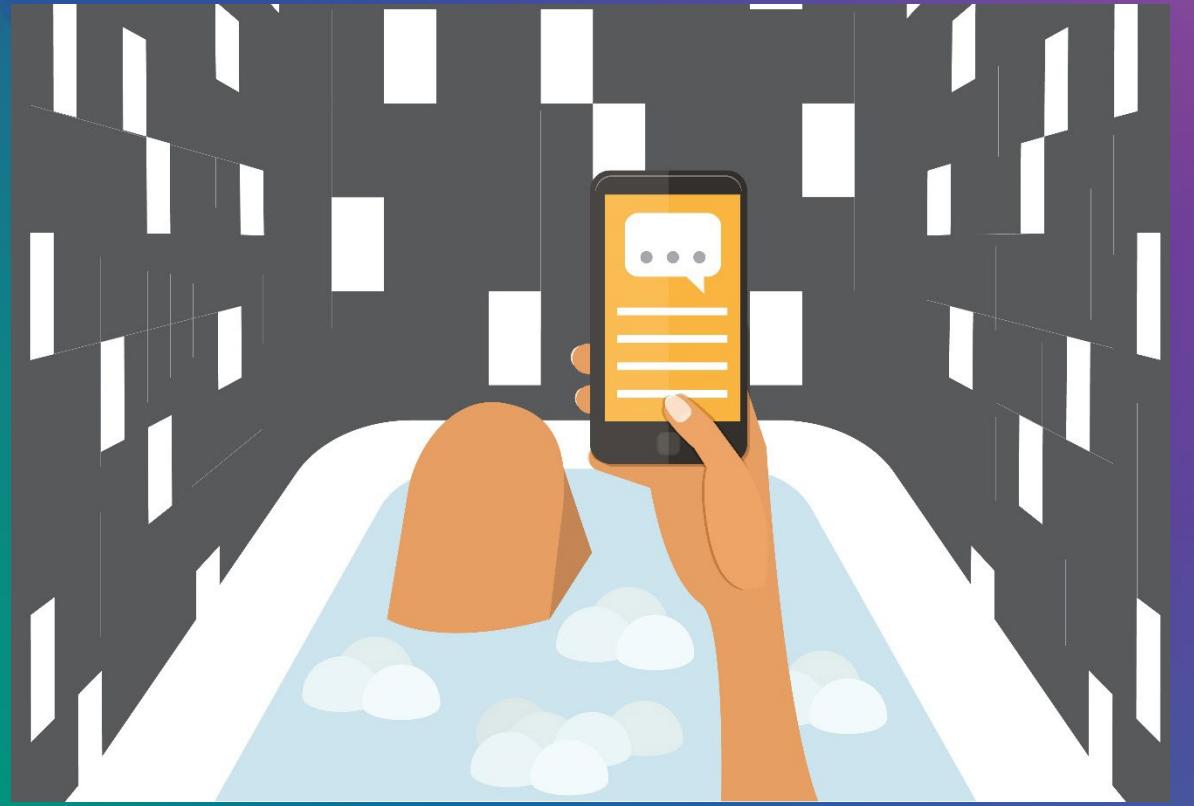


③ 見面前要求購買遊戲點數咁、禮物咁或支付虛擬資產作保證金；其後繼續要求付款



網上援交騙預防及處理

- 網上交友時，要認清對方身份
- 若在見面前被要求繳付保證金，絕大部分都是騙案
- 如接獲恐嚇應報警求助



網上求職騙案

甚麼是刷單？

刷單

店家付款請人**假扮顧客**，用以假亂真的購物方式提高網店的購物方式提高網店的排名和銷量獲得鎖量及好評吸引顧客

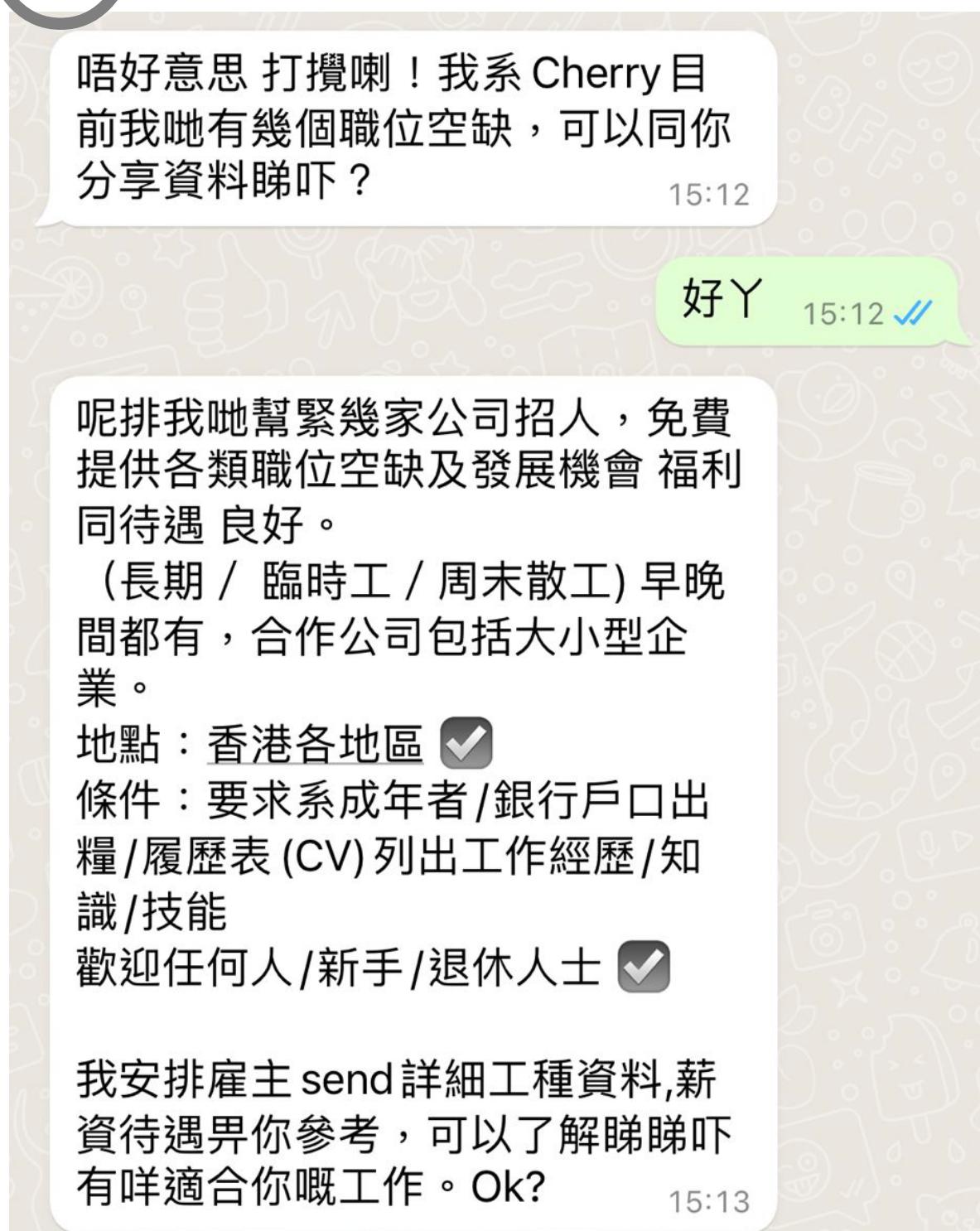
刷單詐騙

騙徒利用**招聘網站**、**兼職群組**等途徑發布虛假兼職訊息，以高額回報為誘餌，套用真實刷單兼職的工作流程，待刷單成功後，再以**系統**、**網絡**、**凍結問題**等藉口，要求受害人多次**匯款**

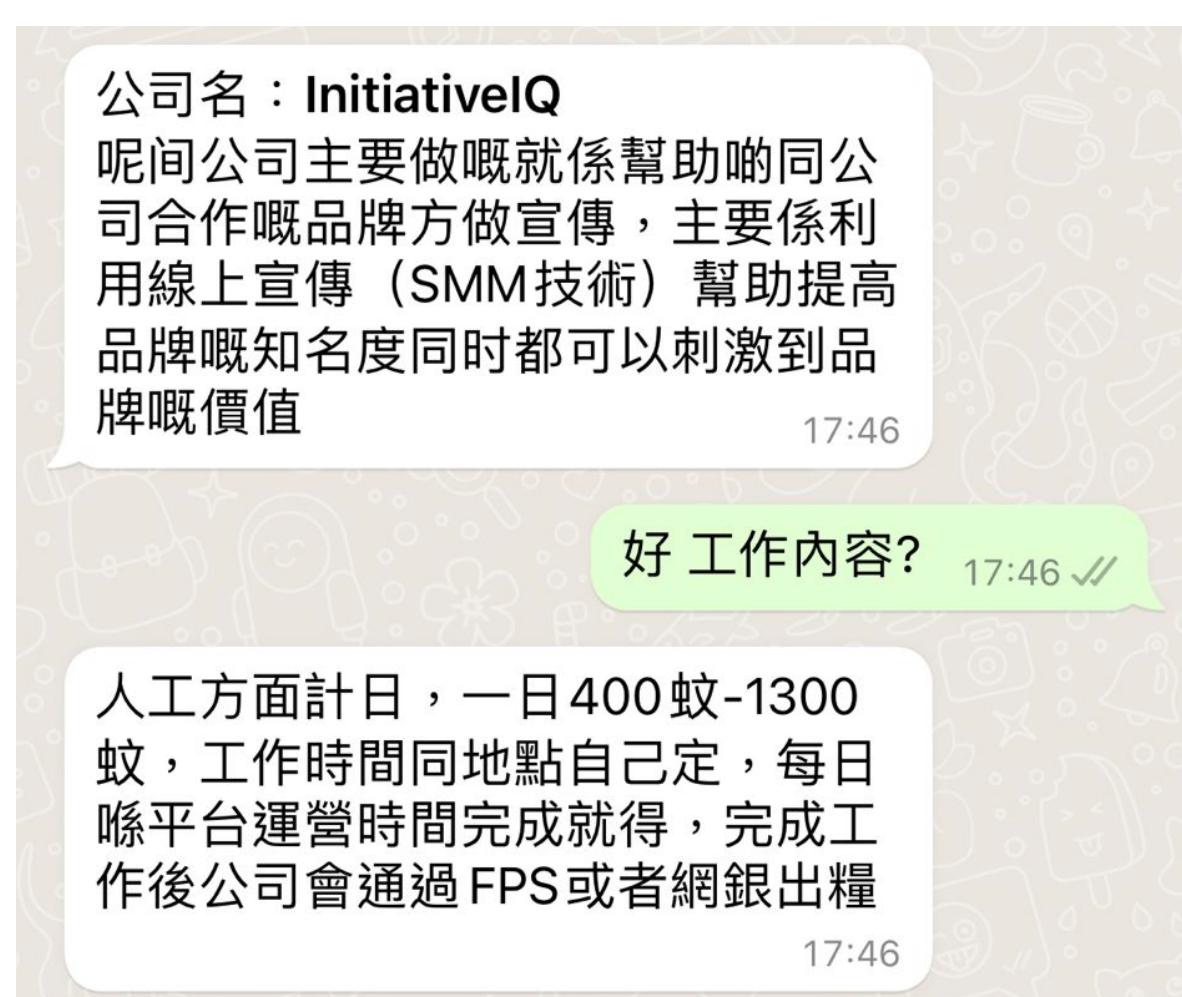


網上求職騙案 - 刷單騙案

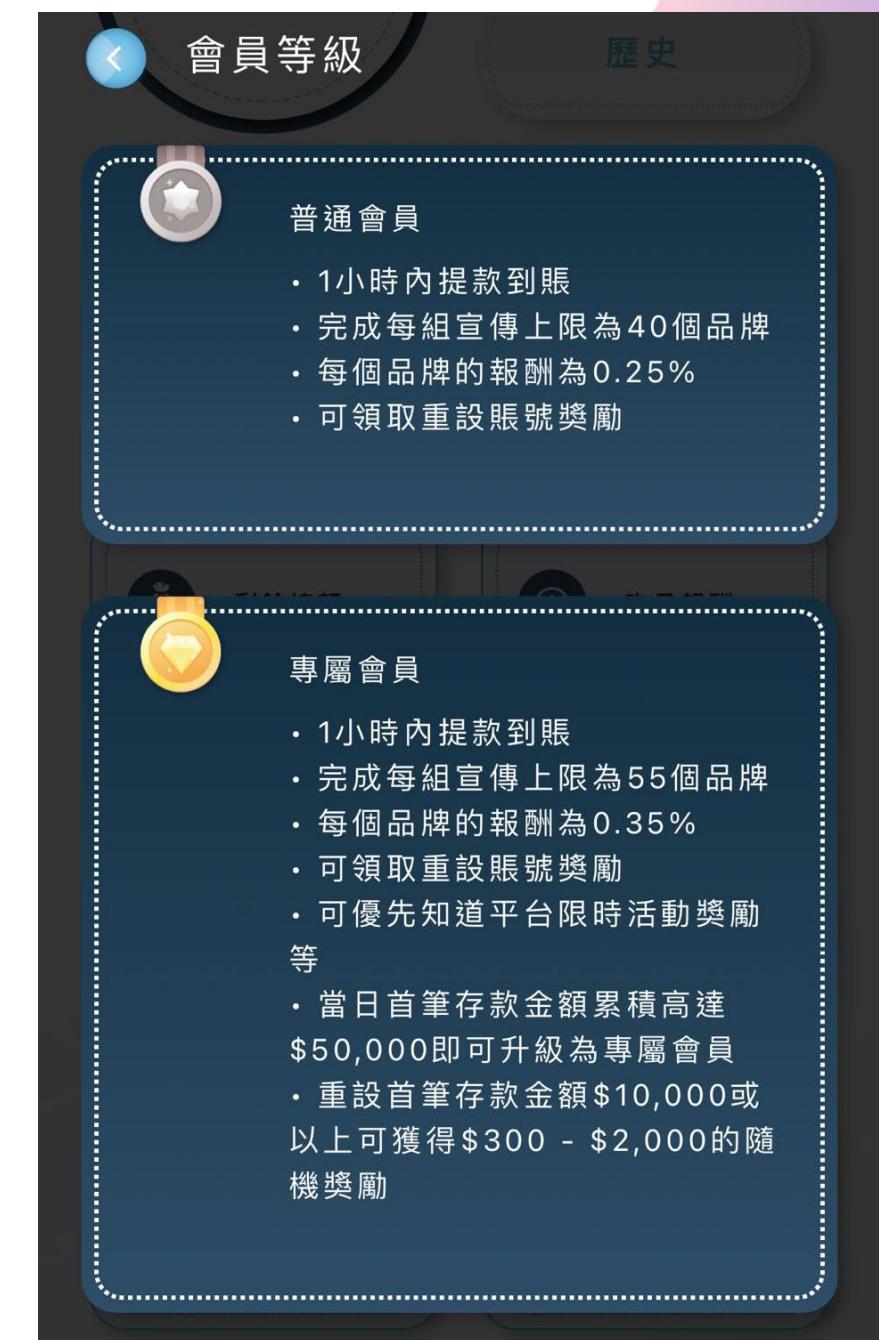
1 白撞訊息介紹職位空缺



2 介紹網上宣傳工作並強調即時出糧



3 虛假網站完成任務後收取「報酬」，存款愈多，比率愈高



網上求職騙案 - 刷單騙案

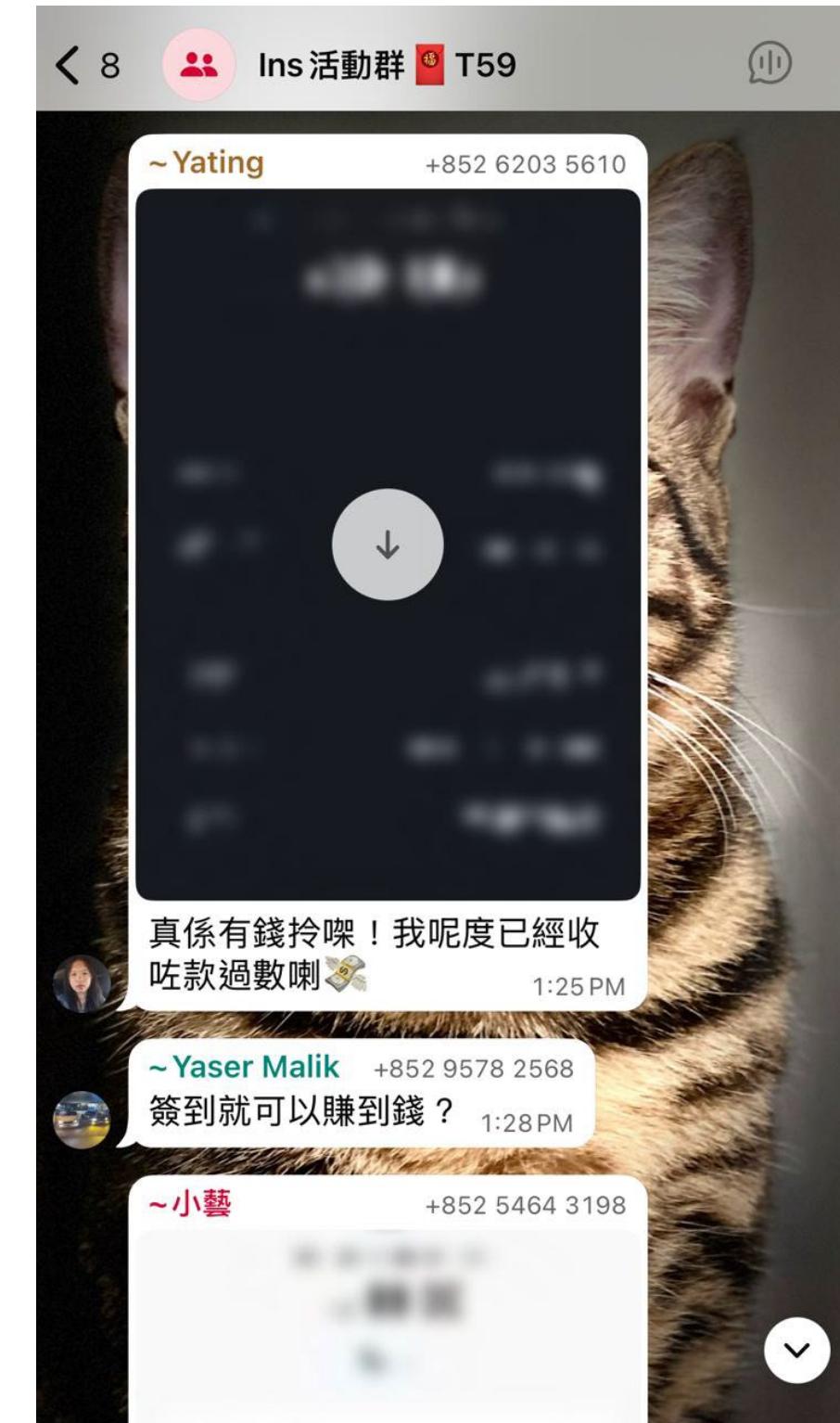
①

拉入不明群組

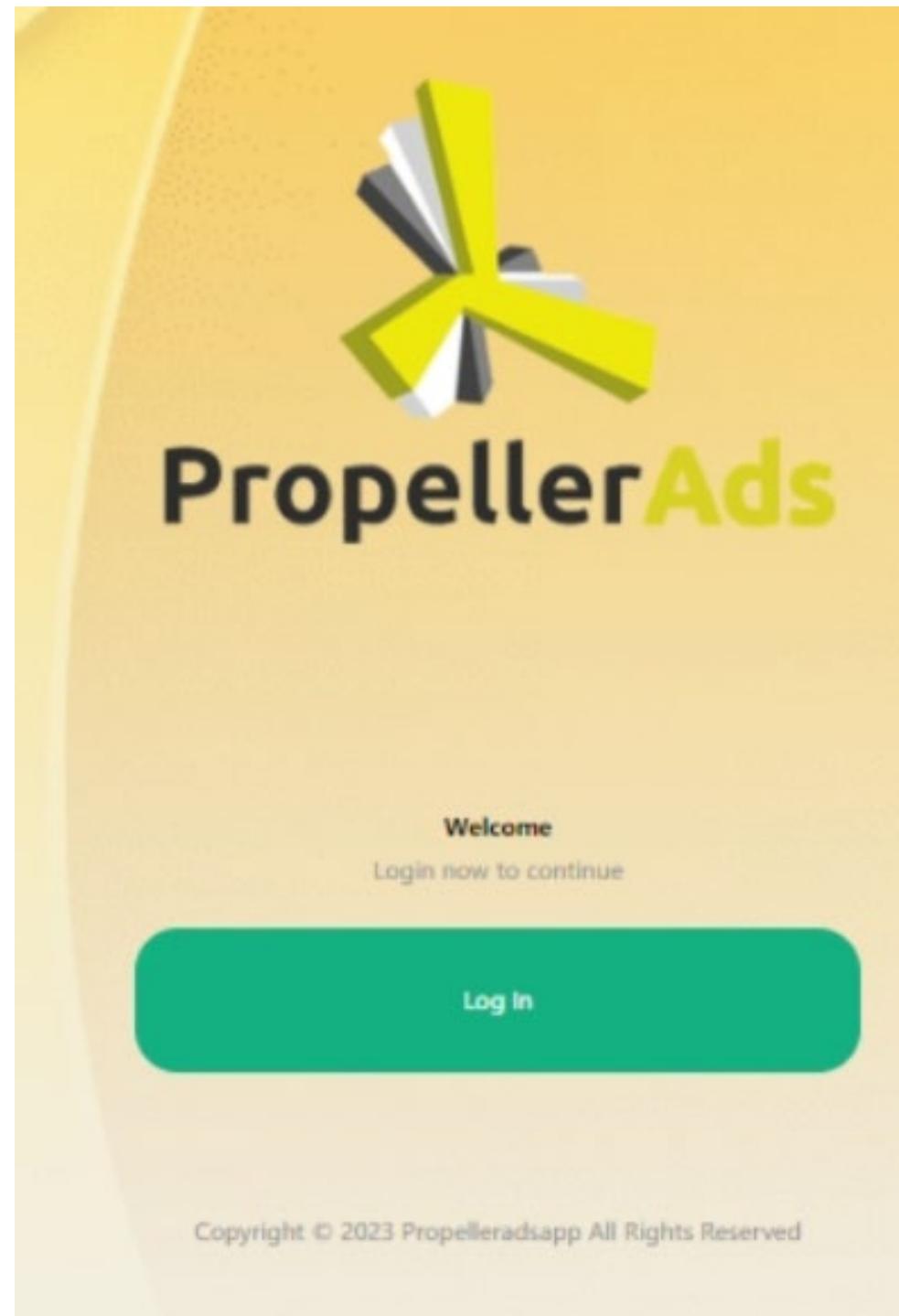
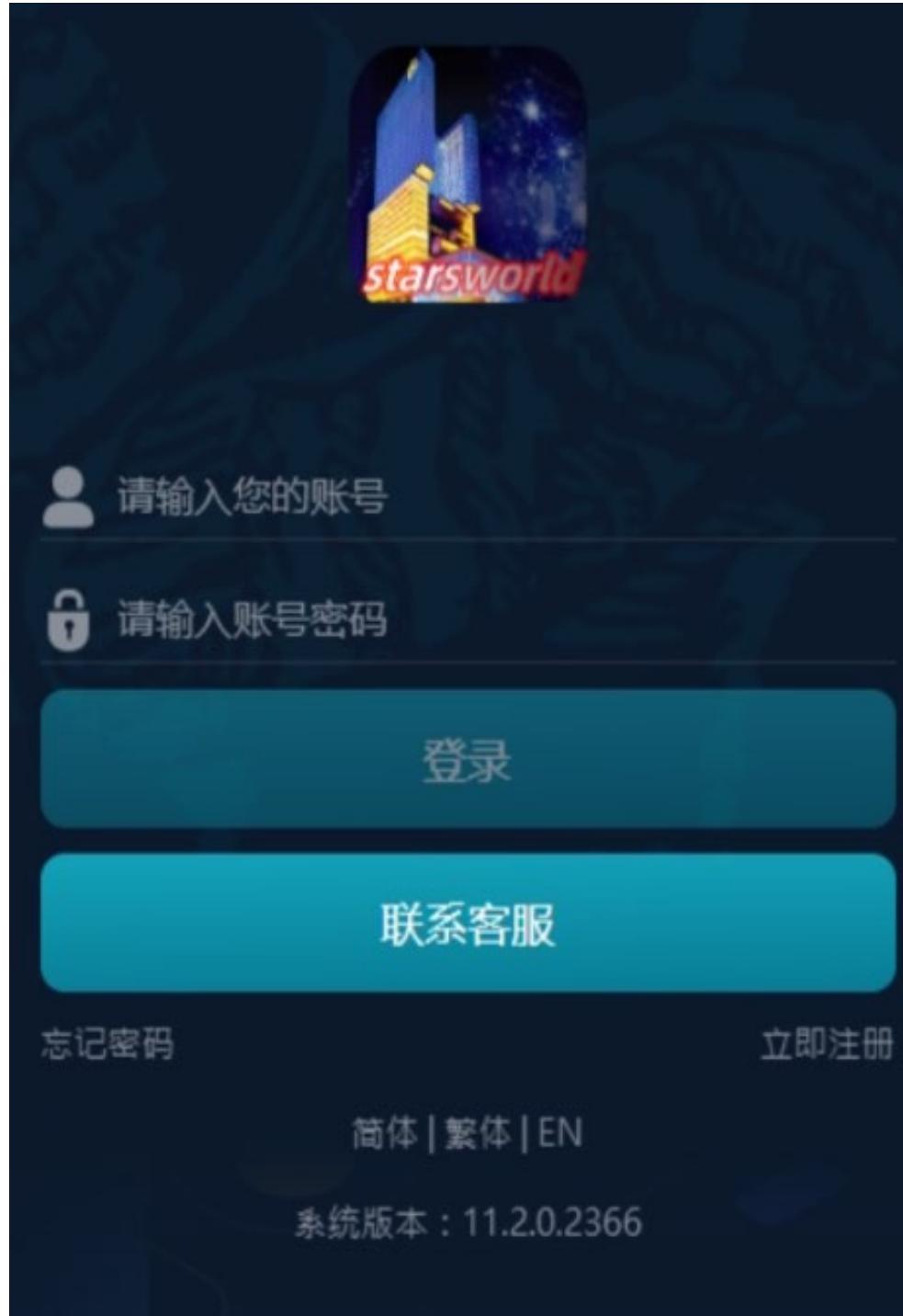


②

偽造獲利截圖



網上求職騙案 · 假刷單平台





人工智能A.I.

人工智能詐騙

人工智能(AI)
模擬人類智能的技術



AI詐騙

- 敏感資訊
 - 相片
 - 金錢

AI詐騙發展趨勢

- 惡意語言模型
- 深偽技術

案例 – AI Deepfake

- 跨國公司財務職員被 Deepfake 視訊會議欺騙
- 騙子預先錄製視頻和音頻，在假會議期間模仿公司高層
- 避免即時交流，使用劇本片段進行單向通信。

Marketing Review

22:06

Take control Pop out Chat People Raise View Notes Apps More Camera Mic Share Leave

Serena Davis Reta Taylor Babak Shammas Danielle Booker

Format Painter Clipboard Font Alignment Protection Numbers Styles Cells Editing Ideas

D11 fx

A B C D E F G H I

Figure 1: Likelihood to Benefit from the Use of Accessible Technology by Type of Difficulty/Impairment among Work-age Adults
* Base: US 18- to 64-years-olds * Source: Study commissioned by Microsoft, conducted by Forrester Research, Inc.

Difficulties and Impairments among Working-Age Adults

The table in Figure 1 represents the numbers of working-age adults (in millions) who have each type of difficulty or impairment defined in the survey.

● : Very Likely ● : Likely

Disability	Likely (millions)	Very Likely (millions)	Total
Visual	27.4	18.5	45.9
Dexterity	31.7	12.0	43.7
Hearing	32.0	4.3	36.3
Cognitive	29.7	3.8	33.5
Speech	4.3	1.9	6.2

Zoom: 125%

Figure 2: Likelihood to Benefit from the Use of Accessible Technology by Type of Difficulty/Impairment among Computer Users

Disability	Likely	Very Likely	Total
Visual	21.9	11.1	33.0
Dexterity	24.4	6.8	31.2
Hearing	24.0	2.5	26.5
Cognitive	19.5	1.7	21.2
Speech	2.5	1.1	3.6

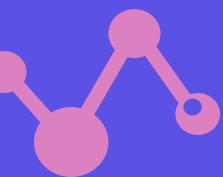
Danielle Booker

74% : People Living with a Disability 26% : People Living with No Disability

The Case for Inclusive Design

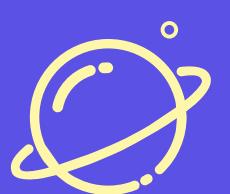
There are 7.4 billion people in the world. Our ambition is to create products that are physically, cognitively, and emotionally appropriate for each of them. It starts with seeing human diversity as a resource for better designs.

Danielle Booker Permanent + Copy Situational Total 26K 1.2M 8M 21M



Deepfake

-
-
-



Deepfake





守網者



守網者
及
防騙視伏APP

守網者：一站式網絡資訊平台

The screenshot shows the homepage of the Cyber Defender website. At the top, there is a navigation bar with links to '網絡常識' (Network Knowledge), '保護你的裝置' (Protect Your Device), '家長及老師' (Parents and Teachers), '網絡罪案' (Cyber Crime), and '資源及活動' (Resources and Activities). The main title '家長及老師' (Parents and Teachers) is displayed prominently. Below it, there is a section titled '不當行為及兒童上網指引' (Guidelines for不当 Behavior and Children's Internet Use) featuring two small images: one of storybooks and another of people on a computer screen. To the left, there is a large graphic with the text '給家長的信' (Letter to Parents) and a grid of words: '性誘識', '兩性價値觀', '關心子女', '網絡活動'. A person is shown sitting at a desk using a computer.



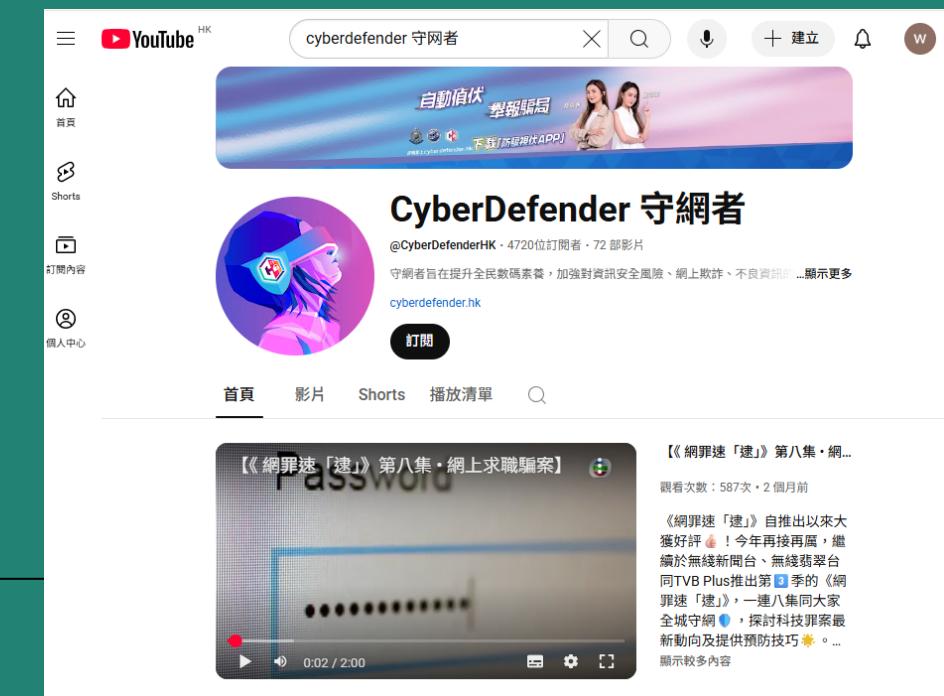
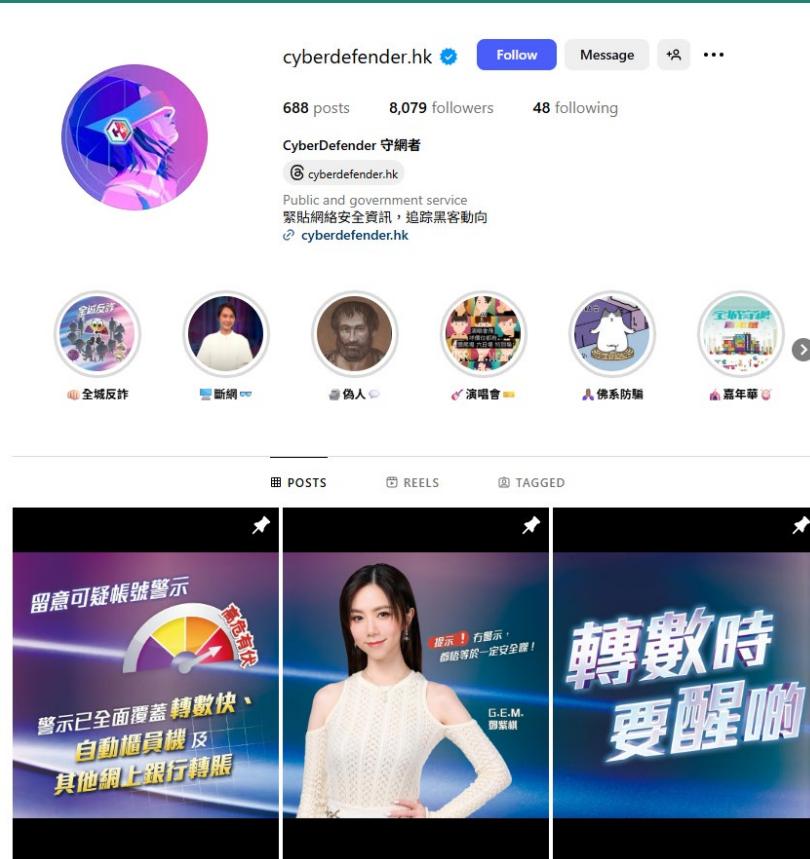
- 為您提供全面網絡、資訊保安、科技罪案防罪資訊

- 引領全城做個醒目數碼公民

CyberDefender.hk



CYBER 守網者 DEFENDER



守網聯盟 (政府部門&公營機構&私人企業)



攝影比賽



快閃活動



社交媒体平台貼文



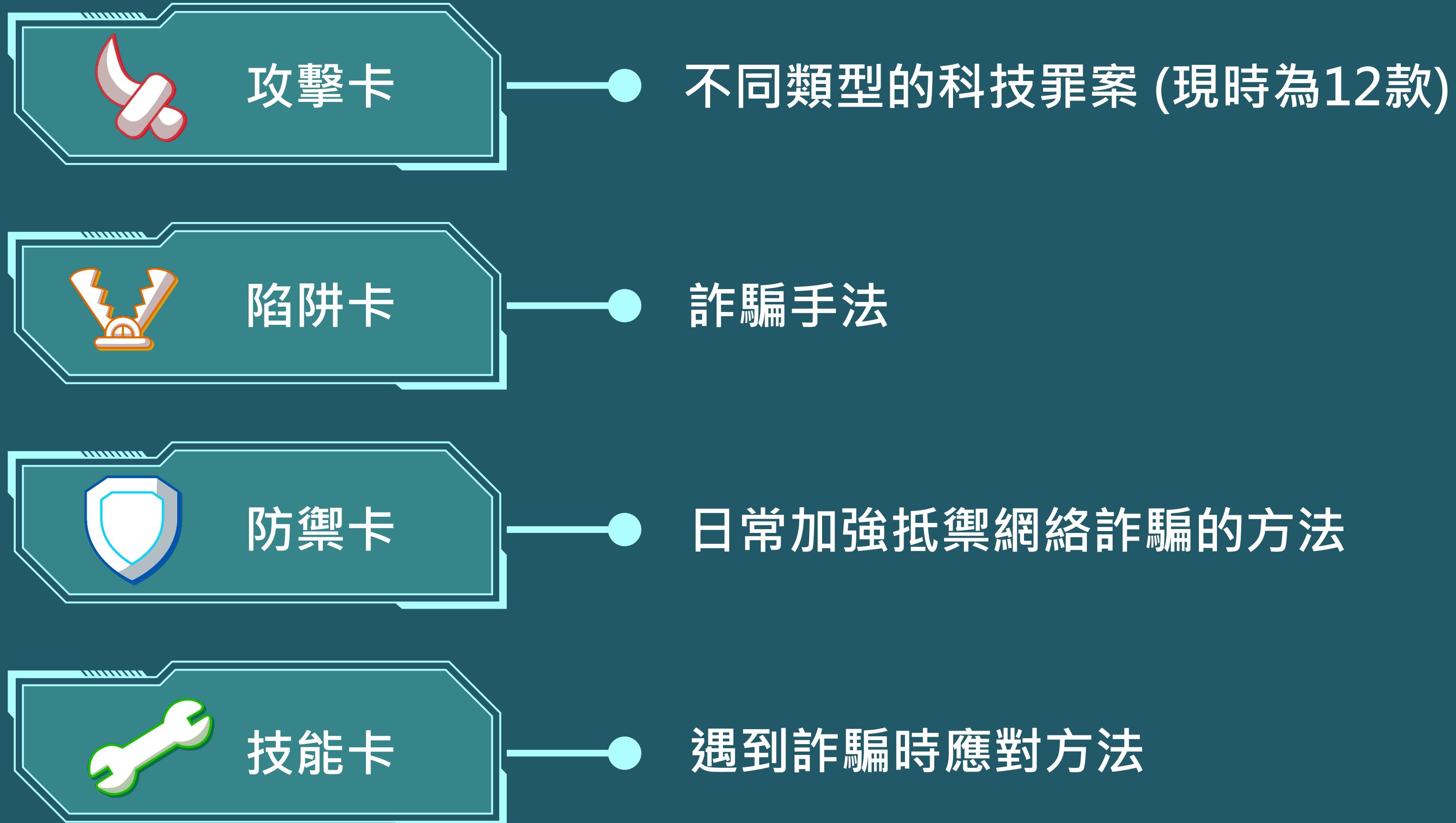
彈出訊息

守網聯盟遊戲卡

- ◆目的: 透過遊戲加深市民對科技罪案的認識
- ◆對象: 高小及中學生
- ◆參與人數: 最少2個，最多6個
- ◆遊戲時間: 20 分鐘
- ◆基礎版全套180張，派發至中小學及青少年中心
- ◆套裝版一套10張(隨機包裝)，於各「守網聯盟」活動派發
- ◆五大等級:
N (Normal , 普通), R (Rare , 稀有), SR (Super Rare , 超稀有), SSR (Specially Super Rare , 特別超級稀有), UR (Ultra Rare , 極稀有)



遊戲卡



攻擊卡



陷阱卡



防禦卡

技能卡



SSR卡

UR卡



防騙視伏器 / 防騙視伏App

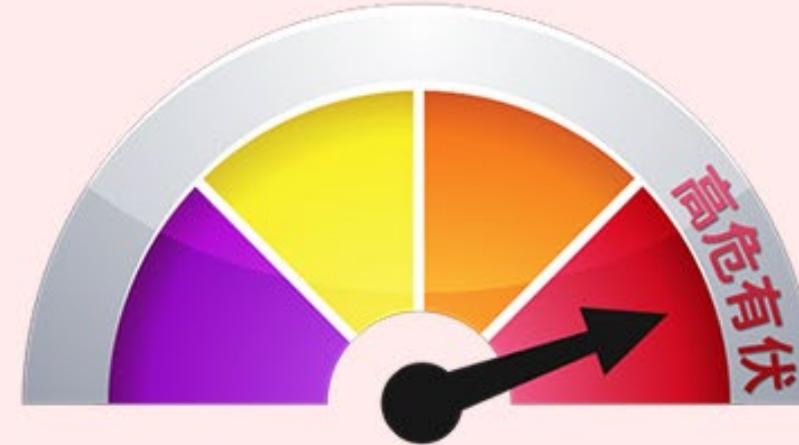
The screenshot shows the homepage of the Anti-Scam Scanner website. At the top, there's a navigation bar with links for 網絡常識 (Network Knowledge), 保護你的裝置 (Protect Your Device), 家長及老師 (Parents and Teachers), 網絡罪案 (Cyber Crime), 資源及活動 (Resources and Activities), 簡 EN, and a search icon. Below the navigation is a banner with two women standing outdoors. The banner text includes "疑似詐騙／網絡陷阱？", "用「防騙視伏器」Check吓啦！", "網址、電郵、電話、平台帳戶、收款賬戶等", and "如不確定資料類型，便無需選擇。". The main headline on the banner is "自動偵伏 爭報騙局" with names "蔡卓妍" and "鍾欣潼" next to them. Below the banner is a call-to-action button: "下載「防騙視伏APP」".



一站式詐騙陷阱搜尋器

防騙視伏器 / 防騙視伏App

搜尋結果



紅色代表「高危有伏」：

輸入的資料與詐騙舉報有關，或網絡安全風險屬高危級別



橙色代表「疑似有伏」：

有相近的詐騙舉報資料，或網絡安全風險屬中高級別



黃色代表「可能有伏」：

你仍需提防中伏



紫色代表「未有記錄」：

但不代表無伏，應時刻保持警惕

防騙視伏App

三大功能



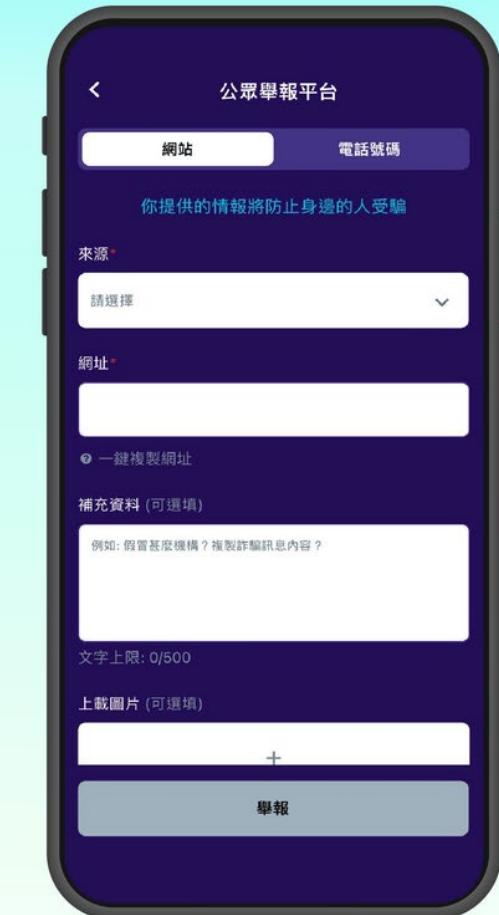
可疑來電警示

此功能自動將你收到的來電與最新的詐騙資料庫作比對，如發現潛在詐騙或網絡安全風險，會即時發出警示提醒你，但你仍可選擇接聽與否。



可疑網站偵測

此功能自動將你瀏覽的網站與最新的詐騙資料庫作比對，如發現潛在詐騙或網絡安全風險，會即時發出通知，建議你不要瀏覽該網站。



公眾舉報平台

當你發現疑似詐騙的網站或電話號碼，可以透過此功能即時舉報。所舉報的資料經分析後可能會被納入詐騙資料庫，供所有用戶使用，以減低其他用戶受騙的風險。

「可疑帳號警示」

G.E.M.
鄧紫棋

留意可疑帳號警示



轉數時 要醒啞

提示！冇警示，
都唔等於一定安全㗎！

警示已全面覆蓋 轉數快、自動櫃員機
及 其他網上銀行轉帳

覆蓋範圍包括：

- 轉數快
- 網上銀行及櫃位轉帳
- 自動櫃員機

Alert

Hong Kong Police Force warning:
The payee account is related to a
scam report.

Please cancel the payment
instruction. Call Police Anti-Scam
Helpline 18222 if in doubt.

Payee

Lee

Bank

The Hongkong and Shanghai
Banking Corporation Limited
(004)

Account

1223054279

Account holder's name

Lee

Cancel

Proceed anyway

「高危警示」！



@HKPolice

打去18222，
逐漸破解騙案又得，
立即破解騙案亦得，得咁



ADCC

Anti-Deception Coordination Centre

反詐騙協調中心



CYBER 守網者
DEFENDER



防騙視伏APP



Download on the
App Store

GET IT ON
Google Play

EXPLORE IT ON
AppGallery