

ADCC
Anti-Deception Coordination Centre
反詐騙協調中心

反擊無限詐術

Understand
FactCheck
Outsmart
理解
查證
智破

全城
防伏手冊

Your Scam

Prevention Manual

終極天書
All answers are
inside

14

種流行詐術 | 特徵 | 防技
14 popular scams X characteristics X prevention techniques

WWW.ADCG.GOV.HK

2026年3月第二版

目錄 防騙熱線一覽

頁數	內容
1	防騙熱線一覽
2	反詐騙協調中心簡介
3-4	騙案排行榜
	本港常見騙案類型
	假冒身份篇
5-8	01 假冒官員
9-12	02 假冒客服
13-14	03 AI換臉(deepfake)騙案
15-16	04 猜猜我是誰
17-19	05 假冒技術支援騙案
	網上交易篇
20-22	06 租屋騙案
23-25	07 釣魚騙案
26-28	08 網上購物騙案
29-30	09 租 / 借 / 賣銀行戶口
	情感利誘篇
31-32	10 裸聊騙案
33-35	11 網上投資騙案
36-38	12 網上情緣騙案
39-41	13 「刷單賺佣」求職騙案
42-44	14 網上求職騙案(賣豬仔)
45	「騙案預警」計劃
46	防騙視伏App

熱線	功能
24小時「防騙易 18222」 諮詢熱線	查詢最新詐騙手法 / 尋求意見 / 舉報案件
緊急熱線 999	情況緊急, 需要即時協助
個人資料私隱專員公署個人 資料防騙熱線 3423 6611	處理懷疑騙取個人資料的 查詢或投訴
香港網絡安全事故協調中心 熱線 8105 6060	接受與網絡保安相關的 事故報告, 包括惡意程式、 網絡釣魚、網上詐騙等
入境事務處「協助在外香港居民 小組」24小時求助電話/ WhatsApp: +852-1868	境外求助
微信求助熱線: 關注「香港入境事務處」 官方帳號, 然後按 「1868求助熱線」聯絡小組	
香港警務處網頁電子報案中心 https://crp.police.gov.hk/crp001/	非緊急報案, 無需警方 即時協助

唔知係咪 **騙案**
就打嚟
18222 問下啦!

HOTLINE



反詐騙協調中心簡介

Anti-Deception Coordination Centre (ADCC)

反詐騙協調中心(ADCC)隸屬香港警務處商業罪案調查科，專門協調警隊各部門打擊及預防詐騙

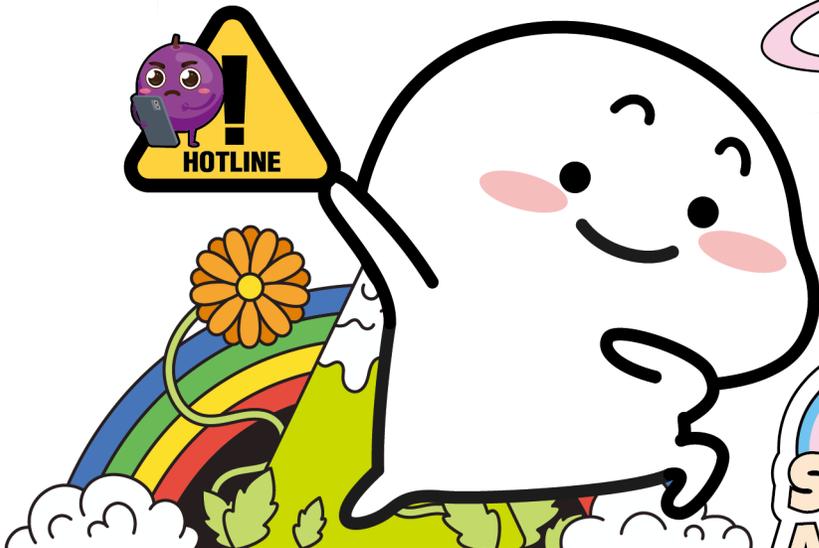
工作重點

制定策略方針 提供電話諮詢 多方協調
推行防騙宣傳 監察騙案趨勢 評估風險

設有24小時「防騙易18222」諮詢熱線

懷疑受騙，就快啲搵我哋啦！

www.adcc.gov.hk





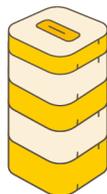
過去 3 年騙案宗數
騙案數字 輕微下跌



+42.6%

+11.7%

-2.9%



2023
39,824宗

2024
44,480宗

2025
43,212宗

騙案 排行 榜





騙案金額 顯著回落

-10.3億



2023
91.8億

2024
91.5億

2025
81.2億 (港元)

www.adcc.gov.hk

騙術排行榜

(2025年以案件宗數計)



第一位

網上購物騙案

第二位

網上投資騙案

第三位

假冒客服騙案



12,505宗

5,135宗

4,440宗

呃錢之最

(2025年以損失金額計)

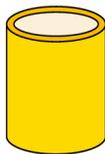
第一位

網上投資騙案

第二位

假冒官員騙案

第三位
刷單騙案



35.8億

8.87億

8.6億 (港元)



01

假冒身份篇

假冒官員

內地公安

來電指控

你犯法？

手法

假扮速遞公司 / 電訊公司 / 銀行 / 政府部門
以預錄語音或真人致電



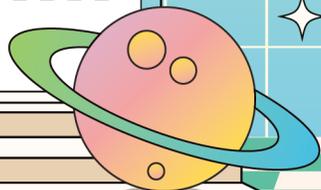
轉駁至假冒內地執法人員
訛稱你：

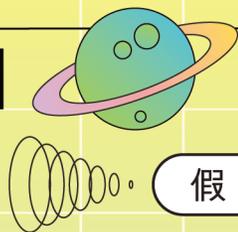
牽涉內地刑事案

開通了新電話號碼，在內地散播危害國安訊息

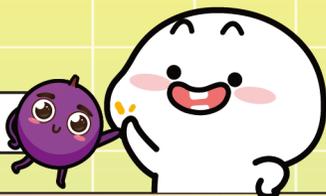


1. 要求轉帳「保證金」至指定戶口
2. 要求下載手機應用程式 (App) 或在假網站
輸入銀行理財密碼，從而轉走你的存款





假冒官員



真實案例 (部分情節經過改動)

法律系學生為千元毀前程

23歲內地來港的碩士生陳小明(化名)某日被一個陌生電話直呼其名。

- 來電者：喂！陳小明，我是電訊公司職員，我們發現你的銀行帳戶有問題！現在轉駁去內地公安部，你積極配合調查吧！
- ★ 小明：什麼？我什麼都沒做呀，我只是個普通學生
轉駁後……
- 來電者：(普通話)你是陳小明？
- ★ 小明：我是……請問我的銀行帳戶有什麼問題呢？
- 來電者：(普通話)你聽着，我們懷疑你和內地一宗洗錢案有關，如果你是清白的話，請配合我們調查，我們只給疑犯一次機會！



來電者要求小明轉帳20萬元「保證金」以示清白，說會在查清資金來源後還給他。小明既驚又恐，對方再突然要求視像通話，接聽後屏幕出現一個身穿「公安制服」的男子，身後白牆赫然有「中國公安部」五個大字。小明還發現他手上有一張「拘捕令」，上面正正寫着自己的名字。

男子用嚴肅語氣向小明認真查問「案情」，指示小明在酒店見面，並叫他簽署「保密協議」。不過，小明愈想愈不對勁：政府部門不是常說不會收保證金嗎？於是致電18222問個究竟。

接報警員順水推舟，在酒店陪小明等候「官員」現身。果然，一名穿西裝的男子主動走近，馬上被警員拘捕，身上被搜獲多份偽造保密協議及偽造公安證件。

結局：

小明沒有任何金錢損失，而被捕西裝男子為就讀法律系的本地大學生，被揭發為了賺取千元報酬而扮演官員行騙，自毀前程。

01

假冒身份篇

假冒官員

特徵

- 身穿仿製公安制服
- 要求轉帳「保證金」
- 偽造拘捕令
- 聲稱幫你證明清白
- 威脅限制出入境
- 要求保密及斷絕與外間聯繫



防技

防騙圖示



- 若來電者自稱「公安」，**立即收線**
- 緊記內地公安或執法機關人員**不會**致電至香港辦案
- 內地公安**絕不會**要求你繳交「保證金」，或提供銀行資料及理財密碼

冒充內地執法人員
見到證件也未必為真

騙上騙



●●● 真實案例 (部分情節經過改動)

受害人變「特務」

騙徒在誘騙受害人轉帳後，會進一步慫恿他們參與所謂「特務行動」，並訛稱完成任務後可取回被騙款項。

曾有受害人深陷假冒官員騙案，為求「贖罪」而同意擔任「特務」，**按照騙徒指示**向其他受害人展示偽造的執法人員證件、假保密令並收取騙款。然而，市民明知而協助騙徒進行犯罪活動，同樣需要**負上法律責任**。



刑責

根據《刑事罪行條例》
任何人使用或管有虛假文書
任何人士如干犯串謀欺詐罪行
一經循公訴程序定罪，
最高可處14年監禁



02

假冒身份篇

假冒客服

電訊商發短訊

要你填資料?

手法

騙徒假扮支付平台/大型企業(例如微信、淘寶、WhatsApp、YouTube、Netflix)/電訊商/銀行的客服致電市民,部分發放釣魚短訊



以不同藉口誘導你回撥電話或點擊釣魚連結

常見藉口:

- 聲稱你有大額保單,即將要以自動轉帳方式繳交保費
- 你有快遞未能派送
- 你曾訂購產品/服務但未付款,或會以月費形式從你戶口扣除



指示輸入網上理財用戶名稱、密碼及驗證碼
然後轉走你的存款



認清 NOTICE

假客服詐騙方程式

假客服



藉口

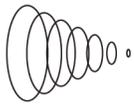


付款

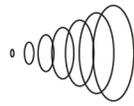
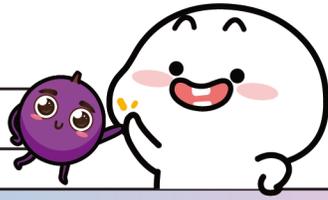


= 呢你錢!

遇到有人自稱支付平台或大型企業客服來電,應提高警覺



假冒客服



真實案例 (部分情節經過改動)

為取消外賣損失4,300元

「你的訂單#12345已確認,扣款1,200元,如有疑問請致電12345678。」

家庭主婦李小依(化名)拿起手機一看,大驚,心想:吃什麼外賣要花1,200元,自己明明沒有叫外賣,怎會有訂單?難道是丈夫的?抑或是外賣App出錯?完全沒理由呀……

為了取消這扣款,小依回撥短訊內的電話號碼找客服。

- 小依:我收到你們的短訊,說我下了1,200元訂單,還已經扣錢,我根本沒有訂過!
- 客服:你好!請問小姐你怎樣稱呼?請提供訂單編號。
- 小依:12345。我姓李。
- 客服:感謝李小姐,我這裡查到你的訂單已獲確認,訂餐餐廳是中環XYZ飯店,你確定沒有下單嗎?
- 小依:沒有,你們肯定出錯,馬上幫我取消扣款。
- 客服:一般而言,我們不可以取消客人已確認的訂單,但在這特別情況下,我可以幫你申請取消,需要三個工作天處理,請提交4,300元保證金。
- 小依:為什麼要付保證金?還那麼多?
- 客服:噢!那只是程序上需要,如果調查結果顯示是我們出錯,會退還所有款項,請放心。
- 小依:唉,那好吧!怎樣交?

於是,小依按客服指示,匯款4,300元到指定銀行帳戶。

結局:

小依其後登入外賣App,卻發現沒有這張訂單,短訊發送人名稱也不像平日般帶有「#」號。小依在App內聯繫真正的客服,才知道自己受騙。



02

假冒身份篇

假冒客服

特徵

發送人名稱沒有以「#」號開頭

可疑連結 官方App無相關通告

要求共享手機畫面

要求輸入網上理財密碼

防技

- 慎防沒有以「#」號開頭的短訊發送人名稱
- 別回撥短訊中的電話或點擊連結
- 致電相關機構熱線核實,而非短訊中的電話

認清!

認住「#」號

避開!



客
服

假客服·藉口·付款

= 呃你錢

假
冒

遇到有人自稱
支付平台或大型企業
客服來電
應提高警覺



香港短訊發送人名稱以「#」號開頭，表示短訊由經官方認證的機構發送。以「#」開頭標示登記名稱，作用是防止假冒、反詐騙及提升短訊可信度。

目前，短訊發送人登記制已涵蓋政府各部門、主要銀行、電訊商等各行各業。

名冊可到通訊事務管理局辦公室網站查核。

迷失「#」

訊息

HSBC

今日下午 2:55

【匯豐銀行】經本人授權體驗騰訊保險將於今日從本行戶口劃扣25920HKD，保單已生效詳情洽保險官網 <https://i-robuor.xyz>

訊息

HOY TV

Text Message - SMS
Today 11:39AM

您已成功續訂 Netflix 家庭版會員服務，月費 HK\$2180.00 若非您本人操作，請您聯系客服取消：30016134

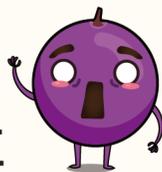
03

假冒身份篇

AI換臉騙案 — ✨ (Deepfake)



股壇神童 在社交媒體



教你投資?

手法 🔍

1. 騙徒利用官員或名人的圖片或錄音，竄改公開片段
 ⚡
 誘騙事主投資
2. 騙徒從社交媒體、視像通話或網上的公開影片取得他人的面容，聲音等生物辨識資料
 ⚡
 通過深度偽造(Deepfake)技術假冒你的親友或同事，或假扮有意發展情緣
 ⚡
 騙取事主金錢及個人資料



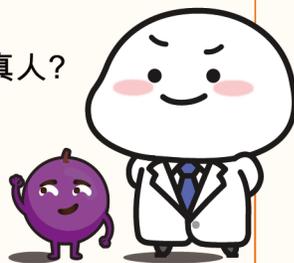
如何辨別影片是利用人工智能(AI)製成?

面部表情不自然	光影效果異常	聲音與口型不匹配
邊緣模糊或變形	背景不穩定	過於完美而顯得不真實

防 技

進行視訊聊天時，如何確認對方是真人?

- 要求對方作出隨機動作
(例如: 用手遮住左眼/舉起三隻手指)
- 檢查聲畫是否同步
- 觀察嘴唇動作與聲音是否一致



AI換臉騙案

真實案例 (部分情節經過改動)

公司「會議」出席者全是Deepfake產物

在一場公司高層視訊「會議」上，賈琛(化名)單獨代表香港分公司出席，他神色凝重，表情緊張。

這是因為他先前收到一封來自海外總公司「財務長」的秘密電郵，「財務長」在電郵告訴賈琛，公司正進行一宗「秘密大額交易」，需要動用香港分公司的資金。賈琛認真細看電郵的用字，的確和財務長寫的一樣。

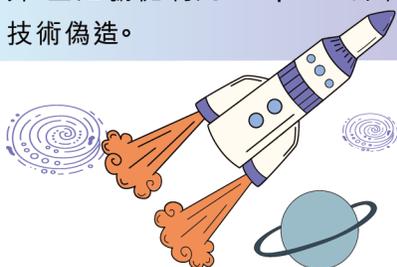
電郵裡附有一個視訊「會議」連結，寫着今日下午二時會有一場高層「會議」，多地分公司都會派「代表」出席。

視訊「會議」接通後，賈琛看到很多熟悉的臉孔，也聽到很多熟悉的聲音，包括總公司的「財務長」和多地分公司的「代表」。「財務長」認真地就電郵裡談到的「秘密交易」向各人作指示。

經過這場視訊「會議」，按「財務長」的指示把總額兩億港元的資金匯到多個指定銀行帳戶。

結局：

賈琛匯款後在一個會議上查詢時，才揭發這是一宗AI換臉騙案。該視訊「會議」的出席者除了賈琛外，全是騙徒利用Deepfake深偽技術偽造。





親戚突然來電

問你 借錢?



手法

1. 打電話與你閒話家常



但不會說出自己是誰

誘導你猜測身份，對方馬上冒認

2. 在 WhatsApp 使用 AI 合成聲線扮作你上司、親戚等身邊人



用各種藉口借錢應急

例子: 被捕急需保釋金 / 代公司墊支轉帳



防技



- 直接詢問對方姓甚名誰
- 試探對方身份是否真確，並可致電其他親友確認
- 遇到借錢或緊急求助，務必冷靜求證





真實案例 (部分情節經過改動)

扮老友論點心

電話響起……

- ▲ 何仁(化名): 喂, 是哪位?
- 來電者: 喂, 好久沒見, 你認不出我嗎?
- ▲ 何仁: 我還真認不出, 你是?
- 來電者: 你可真會說笑, 早陣子我們一起吃過飯。對了, 吃飯沒有?
- ▲ 何仁: 還沒, 正準備去樓下喝茶呢!
- 來電者: 你樓下那家不好吃, 下次和我一起去灣仔水魚茶樓, 那裡的燒賣可好吃了。
- ▲ 何仁: 那家是挺不錯。我跟你去過那家吃嗎?
- 來電者: 我就說嘛。那家是很不錯。除了燒賣, 還有蝦餃、珍珠雞都還可以。
- ▲ 何仁: 對對對, 都還可以。啊……我想起來了, 你是不是老陳的那個朋友?
- 來電者: 不就是我嗎! 你再也不說, 還以為你真認不出來。
- ▲ 何仁: 哈哈, 老了, 記性差多了。怎麼你換了電話號碼? 弄得我以為是詐騙。
- 來電者: 我最近換了電話號碼, 你就認着這個號碼好了。
對了, 老陳的事你聽說了嗎?
- ▲ 何仁: 老陳他怎麼了?
- 來電者: 他最近生意周轉不靈, 你沒聽說嗎?
- ▲ 何仁: 他不是幫人打工嗎? 怎麼會有生意。
- 來電者: 噢, 他沒跟很多人說, 他跟朋友合資做小生意, 怎料那個朋友因為欠債跑路了, 現在差12萬元才可以做下去。我跟其他人已經湊了8萬元幫一下老陳, 你看看要不要也幫他一把。
- ▲ 何仁: 他老是被人當水魚, 也不是第一次了。
- 來電者: 其實他那門小生意還可以的, 就是缺了資金周轉。
- 何仁: 唉……好吧, 老陳也肯定不好意思問人拿錢, 算上我, 我出4萬元吧。
- 來電者: 都說你是老陳最好的兄弟, 那你轉帳到水魚銀行, 帳號是123123456789。由我統一計算, 再轉給他。

結局:

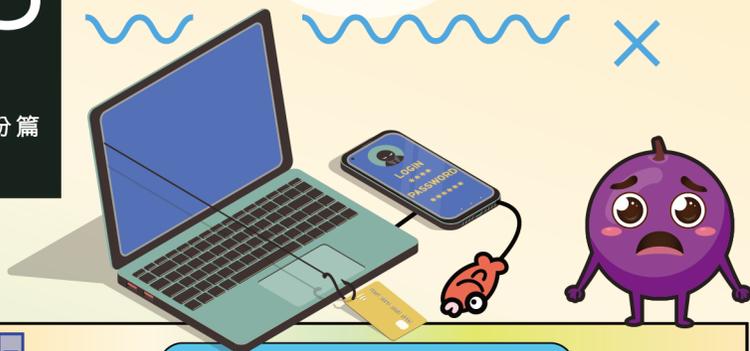
過了一段時間, 何仁相約老陳吃飯, 問起借錢一事, 對方卻說不知情, 亦否認與他人合作做小生意。兩人撥打所謂「老陳朋友」的電話已無人接聽, 驚覺被騙, 遂到警署報案。



05

假冒身份篇

假冒技術支援騙案



在上網時電腦

突然彈出警告視窗?

手法

你瀏覽網站時，畫面突然彈出視窗，顯示電腦中毒警告，附有求助電話號碼，誘騙你致電求助



騙徒假扮電腦技術支援人員接聽電話，要求你下載遠端操控程式，並開放電腦權限



遙距控制你的電腦，聲稱發現違法行為，轉介至假冒警察的騙徒



訛稱要追蹤黑客，指示你在電腦輸入密碼，檢查銀行戶口



騙徒進行「檢查」時，同時竊取銀行理財密碼等個人資料，最後轉走存款



假冒技術支援騙案



真實案例 (部分情節經過改動)



「細心客服」引導入局

退休人士姚小心(化名)在社交平台收到一個好友邀請通知。仔細看過對方的簡介後,她同意了這個好友邀請,誰不知一按下去電腦突然出現當機畫面,並出現了Microsoft Defender的警告:

“ 你的電腦可能正遭受病毒攻擊,請不要作出任何動作,並致電Microsoft團隊以解除封鎖。電話:12345678。 Microsoft 團隊 ”

小心本來打算重新開機,但又看見警告視窗出自Microsoft這家大型軟件公司,想一想覺得還是打電話尋求幫助更好。

接通電話後,小心聽見一把操印度口音的英語聲線,對方介紹自己為Tom Jones,是「Microsoft」的「客戶技術支援專員」。他仔細聆聽小心形容的當機畫面,詳細地向小心說明電腦問題所在。小心對其態度非常滿意,按他建議下載了遠端操控程式,開放權限方便讓他詳細檢查電腦,兩人不知不覺聊了近兩小時。

忽然, Tom Jones 通過聊天軟件發送截圖給小心,表示發現其電腦被黑客入侵,指示小心填寫表格,並指會馬上轉介至香港警方跟進。

小心此時已經有點迷失,只想盡快解鎖電腦,急急填妥表格並發送至指定電郵。果真,她很快便收到電郵回覆,詳列了她的個人資料、案件編號,以及負責調查警員「黃警官」的聯絡資料。

不久後,有一個視訊電話打進來。接通後,一位身穿警服的男子筆直坐着,自稱是「黃警官」,表示小心的電腦涉及國際洗黑錢罪行,指示她在電腦輸入銀行資料,說着電腦便自動跳出銀行登入介面。小心心想這次有大麻煩了,馬上按指示輸入……

結局:

騙徒短時間內便把約500萬元的存款轉走,小心察覺不對勁,前往警署報案,但為時已晚。



05

假冒身份篇

假冒技術支援騙案

特徵

不明來歷警告視窗 聲稱「帳戶遭入侵」

聲稱「問題嚴重」、「帳戶將被凍結」

要求授予遠端操控權

要求你致電客戶服務人員

防 技

- 按 **CTRL** + **ATL** + **DEL**

開啟工作管理員，重新啟動電腦即可

- **切勿隨意下載遠端控制程式**，

或將電腦遠端操控權授予陌生人

- 不要撥打警告視窗的電話號碼





網上交易篇

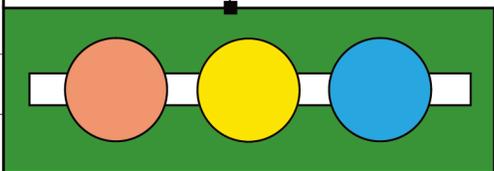
SCAM ALERTS

SCAM



社交媒體 ✨ ✨

出現 超平租盤?



手法 🔍

租客扮作業主轉租物業 /
「假業主」在社交媒體出租假物業



租金異常便宜，甚至使用假相片
吸引你



誘騙預付全年租金

租屋陷阱



SCAM ALERTS

SCAM ALERTS

SCAM ALERTS



「高質樓盤」的真相

內地生蕭虹舒(化名)喜獲獎學金來港讀書,她興奮到馬上在小紅書尋找租房資訊,看到一家「中介公司」的出租單位,月租2萬元,罕有350平方呎的大空間,鄰近學校,還有會所,適合學生租客。

虹舒檢查了一下「中介公司」的小紅書帳號,發現該「中介公司」不單盤源多,單位質素都很高,同時影片也顯示有實體店面,心裡想「心動不如」行動,馬上詢問詳情。

★ 中介: 你好!感謝查詢,這個單位月租18,000元,按香港法規,租戶需要交兩按一上(兩個月按金、一個月上期),如果能以現金一次過繳交一年租金,更可享八折優惠,要不要考慮一下?

● 虹舒: 那就是一次過交226,800元?不用佣金嗎?

★ 中介: 對,佣金全免,還省了四萬多,這價格絕對划算,現在開始旺季了,再晚就可能要租出。

虹舒問了一下父母的意見,他們都傾向一次過交一年租金,讓女兒安穩在港讀書。因怕被其他人租用,所以在沒有先來港看房下,虹舒便將一年租金繳交予「中介公司」。

到了開學季,虹舒一個人帶着兩個大行李箱,提前來港,準備到「中介公司」取鎖匙入住上述單位,才發現該「中介公司」並不存在,驚慌失措的她唯有報警尋求協助。

結局:

警方調查發現涉案「中介公司」並非持牌地產代理,真正的業主也沒有經該「中介公司」放盤,騙徒只是借其照片騙取租金。虹舒為了繼續學業,只好再花一筆錢租房。





▶ SCAM ALERTS ▶▶▶ ●●● SCAM ALERTS ●● SCAM ALERTS ▼

防 技

- 簽署租約時，要留意文件是否正規租約，以及出租人是否真正業主
- 應直接聯絡持牌地產代理，並實地視察物業後再考慮是否租用
- 可向地產代理營業員查詢其全名及牌照號碼，並到地產代理監管局網頁核實對方是否持牌

假文件



騙上騙

租上租



成功入住也被騙？



有受害人通過所謂「中介公司」預付了一年租金，入住了三個月，但其後發現「中介公司」實為二房東，僅僅租下單位三個月，然後「租上租」予受害人，而且收到的租金也沒有交予業主。

SCAM ALERTS

SCAM ALERTS

SCAM ALERTS

SCAM ALERTS

SCAM ALERTS

SCAM ALERTS

▲ SCAM ALERTS ●●● SCAM ALERTS ●●● SCAM ALERTS ▼



機構發短訊



要求你 填資料?

手法

黑客假冒銀行、電訊公司或任何機構設置釣魚網站
外表跟真網站幾乎相同



黑客向大眾發放釣魚電郵或短訊
行文及格式都和上述機構發放的訊息非常相似

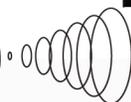
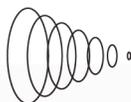


引誘受害人點擊假連結，修正「異常情況」



假連結轉駁到釣魚網站
在受害人輸入個人、信用卡或
網上銀行資料後，騙徒便轉走存款

切勿點擊
可疑連結



● ● ● 真實案例 (部分情節經過改動)

一條短訊投資清零

金融分析師John熱衷投資美股。某日，美股開盤飆升，John全神貫注為客戶整理數據。這時候，手機收到條一看似來自他慣用的投資平台的短訊：



John因太忙，未及細想下點擊連結，網站與他熟悉的投資平台界面無異。他熟練地輸入帳號、密碼和驗證碼，登入後，頁面迅速跳轉至填表界面。John匆匆填完以便盡快「解除凍結」，繼續埋首工作。

他渾然不覺，自己的投資帳戶已悄然落入黑客之手，投資平台App通知功能被暗中關閉，股票已被全數賣出也沒發現。

一日後，John 打開投資平台App查看投資組合表現時瞬間驚呆——他精心買入的優質美股蕩然無存，帳戶僅剩下一堆陌生的冷門股票和衍生產品。他懷疑登入錯誤，反覆核對帳號密碼，終於確信這正是自己的帳戶。

結局：

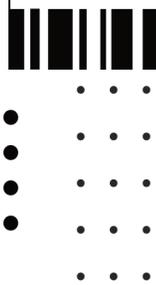
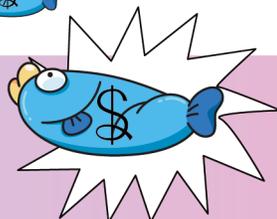
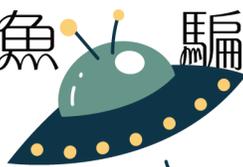
John帳面虧損高達250萬元，及後馬上為帳戶設置多重驗證功能，以策安全。



07

網上交易篇

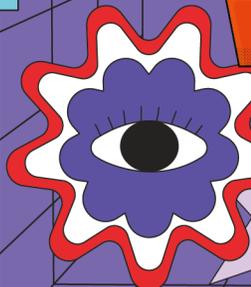
釣魚騙案



防 技

- **直接聯絡** 相關機構確認電郵或短訊是否真實
- **切勿點擊** 可疑電郵或短訊內的連結
- 提防 **沒有以「#」號** 開頭的短訊發送人名稱

CLICK





網上廣告推銷

大額折扣優惠?

手法

騙徒假扮賣家

在社交媒體或買賣網站發貼文或開設專頁，以優惠價、限購等字眼吸引眼球



要求買家先付款後收貨，更只接受以轉帳、轉數快或儲值支付工具付款



在收到款項後失去聯絡

騙徒假扮買家

一：聯絡賣家，聲稱大量購貨/
願意以高價買入貨品



發出虛假收據 - 以虛假入數收據作轉帳證明

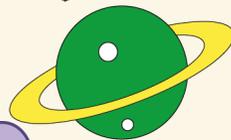


發出無效支票 - 將未能兌現的支票存入賣家戶口，製造虛假入帳記錄



在收貨後失去聯絡

二：假扮已經付款 - 發連結要求你輸入網上銀行資料及一次性密碼，然後轉走你的存款




 網購騙案

真實案例 (部分情節經過改動)

 假期機票買一送一
 

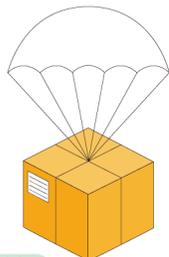
距離復活節還有一個月，汪少飛(化名)的同事在聊假期到哪裡旅行，有的會北上、有的打算去歐洲，他自己則沒有任何計劃。

回到家裡，少飛拖着工作疲憊的身軀，癱軟在沙發上，手指頭機械地滑着手機屏幕。隔了一會，一個廣告吸引了少飛的目光：

【限時優惠先到先得】往來日本香港機票買一送一 復活節假期可用

WhatsApp 電話號碼：12345678

少飛再往下看，廣告帖文只發布了數小時，但已經有幾十個點讚和留言。他馬上打電話給女朋友吳小姐。

- 少飛:BB~復活節想不想一起去旅行?
 - 吳小姐:好呀,我也想去日本逛逛!
 - 少飛:正好,我剛在Facebook看到有機票買一送一優惠。
 - 吳小姐:你這個小傻瓜,沒看ADCC網頁嗎?不少人網上買機票都被騙,先看一下那個廣告帖文的作者資料吧!
 - 少飛:噢,這個作者的帳戶昨天才建立的,真的是騙子!
- 

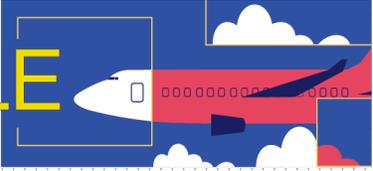
結局:

有女朋友提點的少飛察覺出是騙局，兩人其後改用正規渠道買機票，旅程順利。



Buy get 1

BIG DISCOUNT 機票買一送一

 SALE
 


特徵



超低價格

私下交易

催促付款

假物流單號

假平台或網站

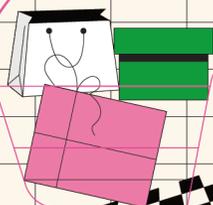
無聯絡方法

防技

 BIG DISCOUNT 機票買一送一

- 銀行戶口的「**可用結餘**」才是反映戶口內可供提取的款項
- 留意網店註冊日期、交易評價及**信譽評級**
- 以**當面交收**或**貨到付款**方式交易，避免通過不明連結交易

SHOPPING DAY



借出銀行戶口

可以賺錢？

提
提
你！洗黑錢是刑事罪行，最高刑罰為罰款
港幣5百萬元及監禁14年

手法

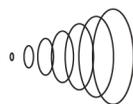
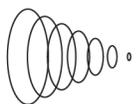
- ① 虛擬交易 – 聲稱作**加密貨幣交易**用途並提供報酬
- ② 求職陷阱 – 標榜「**搵快錢**」，誘使求職者提供銀行戶口
- ③ 明買明賣 – 利誘出租或賣銀行戶口，標榜「**安全不犯法**」
- ④ 網上情緣 – 利用交友App與你發展**網上情侶關係**，取得信任後要求協助開戶

Ⓣ

騙徒利用銀行戶口作傀儡戶口，以**清洗黑錢**

切勿貪心 × 以免墮入圈套

被不法分子利用



真實案例 (部分情節經過改動)

8,000元的誘惑

17歲的伍浩信(化名)已不能登入網上銀行帳戶,一邊盯着手上的一疊鈔票,一邊陷入了沉思。

一周前……

浩信受同學邀請去唱卡拉OK,但因已花光零用錢,所以藉口說有事不去了。一名死黨看出了他的心思,在他耳邊說:「放心,有大哥請客。」

到了卡拉OK店,浩信發現有幾個不認識的人,一身潮流名牌,死黨介紹說這幾位都是做兼職認識的同事,都很會賺錢。一群人唱着唱着很快就熟絡起來,而浩信也耐不住好奇心……

- 浩信:你做什麼兼職呀?為什麼你的同事看起來都那麼有錢?
- 死黨:其實也算不上工作,他們只是借我的銀行戶口去炒幣,定期給我一筆出租費。
- 浩信:多少錢呀?
- 死黨:8,000元。
- 浩信:嘩!這麼多,合法的嗎?
- 死黨:當然合法,都不知道多少人炒幣致富了,而且他們比你更注重資金安全,存一大筆錢在你戶口之前,都要求你先提交身份和住址證明。
- 浩信:我也想加入,可以幫我介紹嗎?
- 死黨:這……好吧,我幫你問一問。

結局:

浩信以8,000元出租銀行戶口,一年後被警方拘捕。因為其戶口被查出涉及清洗500萬元犯罪得益,區域法院經審訊後裁定他罪名成立,判囚42個月。



10

情感利誘篇

裸聊騙案



交友App



新相識要你



下載程式?

結識受害人 ♥ 聊天建立信任

手法

通過社交媒體、交友App或即時通訊軟件結識你，藉聊天建立信任



引誘你進行裸聊及**下載惡意程式**，以盜取通訊錄資料



拍下裸聊片段，**威脅傳至你的親友**，並要求匯款到指定戶口，或以加密貨幣或點數卡支付款項

防技

- **切勿** 在進行視像聊天期間裸露身體
- **切勿** 點擊不明來歷的連結或下載程式
- **切勿** 輕信對方是以「真面目」示人





裸聊騙案



真實案例 (部分情節經過改動)

可愛女孩瞬間變臉

17歲的林一夏(化名)剛剛失戀,某天晚上在網上交友平台尋覓聊天對象時,匹配到了一位叫「小雅」的文青女孩。她的頭像是一張清純的笑臉,自我介紹寫着「喜歡看電影,尋找有共鳴的靈魂」。

聊天記錄

- 
- ★ 小雅:Hi,好久沒遇到香港男生了,你平時喜歡做什麼呀?
 - ♥ 一夏:Hello!我平時就看看Netflix,偶爾打打遊戲。你呢?
 - ★ 小雅:我超愛看電影!最近在追一部懸疑劇,緊張得我晚上都不敢一個人睡,你喜歡什麼類型的電影?
 - ♥ 一夏:懸疑片我也喜歡!最近看了《消失的她》,覺得還不錯。你有推薦嗎?

兩人話題慢慢從電影擴展到生活,輕鬆又愉快。聊到第三天,小雅突然提議視像聊天,並發來一個連結,說是一個平台的私人房間,保證私隱有保障。一夏點擊進去,小雅出現在熒幕上,樣子跟頭像差不多,完全沒有「照騙」。

- ★ 小雅:哈哈,看到你了!好帥哦!要不要放鬆一點,我們玩點刺激的?
- ♥ 一夏:刺激?什麼意思?
- ★ 小雅:嘻嘻,比如.....我們玩個遊戲,誰輸了就脫一件衣服,敢不敢?

那天晚上,兩人聊了快一個小時,畫面越來越大膽。視像突然中斷,小雅發來一段三分鐘的影片,竟然就是剛剛裸聊的畫面!

- ★ 小雅:不要生氣!小妹想賺點生活費,轉5,000元給我就把影片刪了,要不然我就把影片傳給你的朋友、家人,並上載到互聯網。

一夏整個人愣住了,心臟狂跳,嘗試問小雅為什麼要詐騙他,是不是受人威脅等。小雅沒有回應,只是再度要求他轉帳。焦急的一夏把自己的零用錢都轉帳給她了。正當以為事情可以告一段落,小雅再以「刪除手續費」為由,要他再轉2萬元,並不斷用言語威脅他……

結局:

一夏偷用父母手機在網上銀行轉帳時被父母發現,再三詢問之下,一夏向父母坦承錯誤,馬上到警署報案求助。除了一開始的5,000元外,沒有更多損失。

11

情感利誘篇

網上投資騙案

突然被拉入WhatsApp

投資群組?

手法

騙徒通過社交媒體宣傳，聲稱有內幕貼士，假扮專家教投資或隨機拉攏市民加入WhatsApp「投資教學」群組



偽造交易獲利記錄，在群組分享「獲利截圖」，游說安裝虛假投資平台App



騙徒偽裝成客服人員，要求你提交個人資料及轉帳至指定銀行戶口



初期給予你小額回報，目的是吸引你加大投資額



你欲提取資金時，客服人員用各種藉口拖延付款，甚至要求支付大額手續費；最終你無法取回任何資金

認清 NOTICE

注意 白撞訊息叫你投資



情感利誘篇



網上投資騙案



真實案例 (部分情節經過改動)

「投資名人」貼身教學

余青凌(化名)是中學教師,存了可觀的積蓄,最近股市復熾,加上看了許多投資專家的YouTube影片,因而一直留意有沒有投資良機。

某日,她被陌生人拉進一個WhatsApp群組,名為「流大師AI投資教學谷」,群組內有多達180人。她被拉進去時,群組成員已經聊個不停,所有人都稱讚大師的預測專業,還有人貼出截圖,說自己每天都賺7%。

「一天7%,才不信呢!」青凌心想這肯定是詐騙群組,不過她抱着好奇心沒有刪掉群組,默默地觀察。隔天,群組管理員流大師的發言改變了她的想法……

- 大師: 各位投資界朋友,小弟已經連續兩周成功預測每天會升7%以上的股票,你們肯定好奇我是怎樣做到?其實不是小弟厲害,現在股票預測已經是電腦超越人腦的時代了。我所用的是最新人工智能,它能批量分析每天的金融市場消息,看出人類難以理解的細節,從而準確預測股票走向。大家要記住股票市場其實就是一場心理學博奕,AI既能吸收大量資訊,又能理性分析這些資訊,必定更勝一籌。
- 群組成員A: 感謝大師分享,那AI投資會有風險嗎?
- 大師: 任何投資都有風險,關鍵在於使用AI能大大把風險降低。
- ★ 群組成員B: 大師推薦什麼投資平台?
- 大師: 市面上很多流通的投資工具沒有AI功能,所以我個人推薦使用這個「AI貓貓投資平台」。

青凌對流大師改觀,覺得他不像其他投資專家一樣,一味吹捧自己,甚至很盡力教育成員AI投資的好與壞。青凌還發現原來流大師曾經上過電視財經節目,是響當當的投資專家。

不久後,群組管理員私訊青凌,問她有沒有興趣加入「流大師粉絲專屬貼士群」,並說流大師會提供在AI貓貓投資平台投資的專業意見。青凌感覺可以小試牛刀,便按連結指示下載投資App和注資10萬元。

果真,青凌隔兩天賺了三萬多元,其後再充值,愈充愈多……

結局:

青凌眼看已經賺了三千多萬元便想提款,怎料遭客服拒絕,更被要求提交500萬元保證金,青凌拒絕,自此無法登入該App,遂報警求助,終於醒覺是騙徒冒充投資界名人混水摸魚。



11

情感利誘篇

特徵

高回報低風險承諾

平台無註冊或認證

無法提款

不斷誘導追加資金

盈利短期大幅上漲



防技

- 到 **證券及期貨事務監察委員會網站** 查證投資平台的背景及註冊資訊：

https://www.sfc.hk/TC/Alert_List

- 作大額投資前先諮詢專業人士（例如律師或金融顧問）
- 避免通過社交媒體或陌生網站尋覓投資機會



認清楚

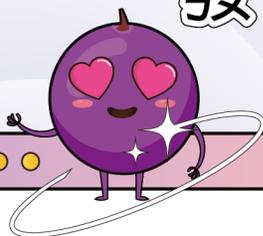
邊有咁大隻蛤姆隨街跳

注意白撞訊息叫你投資



向對象快速

發動追求攻勢？



用「高富帥」、「白富美」或「專業人士」

的相片做頭像，在社交媒體或交友App尋找目標

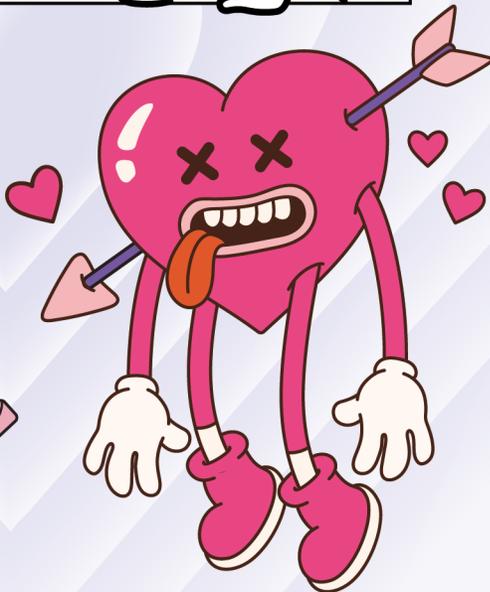


發動追求攻勢，建立網上戀人關係，

然後用各種藉口騙財

例子：

- 突然急需繳付巨額醫療費
- 寄出的貴重禮物被扣查，需要清關費
- 答應見面，但要求墊支行程費用
(例如：機票費用)





真實案例 (部分情節經過改動)

忘年的漏水情緣



「你好,我姓王的,剛搬來你樓下住,發現天花板有點漏水,所以從管理處取得你的電話並聯絡你,希望能和你商量一下。」林近麟(化名)退休多年,收到這則短訊後甚是疑惑,原因是自己和樓下鄰居陳先生一家認識多年,未聽過他們要搬走。



「你是陳先生的租客嗎?」問畢,對方沉默良久。

「噢,看來我搞錯電話號碼了,我剛從新加坡來香港工作,要辦的事情太多了,人生路不熟,忙中有錯,對不起了,打擾了這位大哥。」

這番話讓近麟想起當年自己也是隻身來港,經歷各種風吹雨打才有了現在的生活。

「絕無打擾,小事一宗,王小姐一個人來香港辛苦了。小姓林,既然有緣,王小姐如在香港遇到什麼難題,不妨與我分享解憂。」

「謝謝你,林大哥,我叫王薰,你是我來香港後遇上的第一個好人。」



光陰似箭,一個月過去了,兩人沒有因年齡差異而有隔閡,感情發展飛快。近麟尤其欣賞王薰堅強獨立,而王薰也對林大哥打開心窗,互生情愫,在某一次愉快的聊天中承認了這段忘年戀。

「你明知我對你動了情……要聽話,好好珍惜我。」

又過了一個月,兩人偶爾聊到投資,發現大家想法有很大分別。



近麟: 股神巴巴特也說寧願買磚頭,都不買比比幣。



王薰: 林大哥,他這麼說證明他太老派了,現在一枚比比幣都值好幾間房子了。



近麟: 真的嗎?



王薰: 你不信我嗎?我在交易所工作,對這些最清楚了。我發給你一則新聞,你看看就懂了。如果我現在有一筆錢,肯定會投資比比幣,這樣以後就可以整天陪你,不用工作了。」



該則新聞報道,加密貨幣近年價值倍增,已造就許多人一夜暴富,近麟慢慢認同王薰的想法,更在她的指導下用退休金學習投資加密貨幣。

結局:

近麟多次轉帳至不同銀行帳戶,而銀行職員發現其中一個帳戶有可疑,隨即通知反詐騙協調中心揭發騙局。至此,近麟已被騙約320萬元。

特 徵

完美人設

拒絕親身見面

快速建立親密關係

拒絕視像通話

情緒勒索

突然急需金錢



ROMANCE SCAM



防 技



- 要求與對方進行 **視像通話**
- 利用 **搜尋器** 查看對方相片確認來源
- 通過不同方法 (社交媒體、視像通話) 查證身份，留意言行是否一致



「刷單賺佣」求職騙案 — ✨

WhatsApp 群組教你

做任務賺錢?

手法 🔍



在社交媒體刊登廣告 招聘「點讚員」或「下單員」



聲稱 只需以購物催谷銷量便能抽佣賺錢



要求你先墊支購物款項
並將款項存入指定銀行戶口

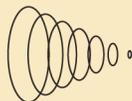


在交易初期，騙徒或發放少許佣金，令人信以為真，再指示墊支更多金錢，最後失去聯絡

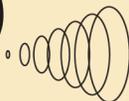




情感利誘篇



「刷單賺佣」求職騙案



找一份兼職竟被騙二次

市道不景氣，薛清江（化名）最近在網上留意有沒有兼職適合自己。清江原本只是想找周末侍應的空缺，但一個廣告吸引了他的目光：

你是否厭倦了朝九晚五的工作？

我們來自大型購物平台XYZ Mall，現誠聘以下職位：

刷單員

- 日薪1,000至2,000元
- 無需經驗，在家工作，只需操作手機
- 專業培訓，只要你肯學，保證教你上手

有興趣請加WhatsApp: 12345678



清江沒試過在家工作，不過自認勤奮好學，覺得既然有培訓，那就可以一試。於是，清江經WhatsApp加入了一個二百多人的聊天群組。

群組管理員介紹稱，刷單員的職責是幫公司下單購買電器，製造更多單數，讓產品看起來更受歡迎，完成後公司會立即退回本金和10%佣金，也就是說買的貨品愈貴，回佣愈多。清江看見群組成員不停分享賺錢截圖，又有熱心成員私下發訊息游說，使用數十元買小電器試試，很快就獲得全額退款和二十多元佣金。

清江態度瞬間積極起來，不停參加刷單任務，購買總值超過20萬元的電器，卻換來群組管理員指責「操作不當，拒絕退款」。清江氣得報警，證實是遭到詐騙。

三周後，清江仍為此憤憤不平，偶爾在社交媒體上看到一個律師廣告，「專業地為被騙人士追討賠償，不成功不收費」，清江二話不說，馬上聯絡「律師」。

不久後，「律師」親自致電清江，指自己追蹤到騙款被匯到澳門一間賭場，現在清江需要立即交20萬元保證金予賭場以凍結騙款，否則賭場不會幫助他，款項再追查不了。

結局：

清江情急之下再付20萬元積蓄予假扮律師的騙子，慘遭二次詐騙，花清光積蓄才報警求助。

情感利誘篇

特徵

經驗及學歷不拘

以簡單任務開始

只用社交媒體帳戶聯絡

拒絕發還本金

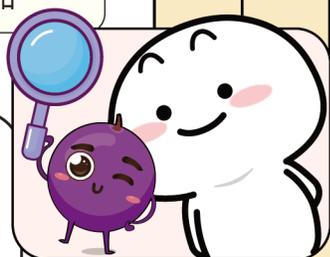
要求先墊支款項

失去聯絡



防技

- 不要相信聲稱職位不拘學歷或經驗，但可享高薪的招聘廣告
- 通過可**信賴的求職途徑**搵工
- 應聘前先了解**公司背景及業務性質**



騙人招聘



認清 NOTICE

刷單任務 = 破產之路



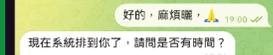
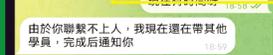
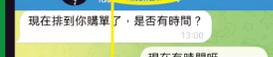
1. 陌生

群組名稱包含大型機構名字



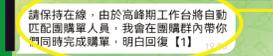
2. 虛構

專業客服人員名稱



3. 假扮

客服系統自動回覆



3 伎倆令你鬆懈

WhatsApp 陌生訊息

14

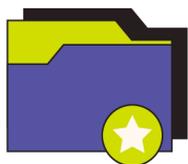
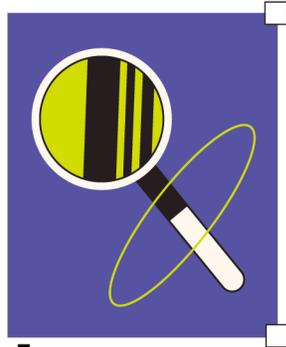
情感利誘篇

網上求職騙案(賣豬仔) ✦

東南亞公司

請你出任

高薪厚職?



JOB 苟工
HUNTING



騙徒在社交媒體或娛樂場所尋找目標 ✦



邀請你到外地工作，標榜「東南亞高薪厚職工作」

「無需學歷或工作經驗」「包機票食宿」



抵達後被沒收護照及手提電話



被不法集團販賣到詐騙園區從事詐騙工作
可能受到身體虐待甚至失去性命 ✦





真實案例(部分情節經過改動)

恐怖免費旅行



年輕貌美的宋小珠是「月光族」，有錢就花，沒有積蓄，閒時喜愛到酒吧裡喝喝酒聊聊天。某日，她在酒吧通過朋友認識了一個大自己幾年、姓郭的女人，對方一來就請她喝酒，揮金如土，極像富家大小姐。

小珠想着有「免費午餐」那麼好，就多次主動上前示好，又不停敬酒給郭小姐，說好話，哄得她非常開心。郭小姐在酒局後帶着酒勁抱小珠，唸唸有詞地說想繼續喝，不想離開小珠身邊，甚至說要請小珠明天一起去旅行。

起初，小珠以為郭小姐只是開玩笑，豈料下一秒她真的問小珠拿身份資料，用手機買機票。小珠頓時不知如何是好，想勸阻郭小姐，卻被她一手擋開，說「你明天拿行李來機場就好，我會照顧好你。」

第二天，小珠半信半疑地拖着行李到機場，竟然真的看到郭小姐笑着走來，說要帶她離開香港好好放鬆，「別想那些鬼東西了，人生太短，要努力讓自己開心，我以後叫你妹妹，好不好？」小珠開心地笑了。

下機後，小珠跟着郭小姐走，突然兩名男子走來強行抓住她，搶走她的護照及手機後把她抱起帶上一輛私家車。小珠一路掙扎大叫，附近卻奇怪沒有什麼人，郭小姐轉眼也不見了。

結局：

小珠被送到詐騙園區從事詐騙工作，幸未曾受到虐待，最後獲釋。警方以串謀詐騙罪拘捕郭小姐，原來其職業是美容師，為了賺錢參與人口販賣，四處尋找獵物。



特 徵

高度
風險

高薪厚職

職責說明模糊

沒收護照

限制自由

快速錄取

包機票食宿

防 技

- **切勿輕信**「高薪厚職」、「無需學歷或工作經驗」、「包機票食宿」等「賺快錢」的機會

- 與親友 **保持聯繫**，告知具體地點及行程

- 入境事務處「協助在外香港居民小組」

24小時求助電話：
+852-1868

- 微信求助：關注「香港入境事務處」官方帳號，然後按「**1868求助熱線**」聯絡小組

核實公司資料

「騙案預警」計劃

反詐騙協調中心聯同銀行持續監測可疑交易與銀行戶口，一旦市民轉帳至可疑銀行戶口，「防騙預警」便會啟動，由銀行職員或警方告誡市民停止可疑交易。

我們會向潛在受害人：

發出警示短訊 | 派警員上門提醒 | 致電作警示
在這個時候，你應該立即停止可疑轉帳或交易，並提高警惕。



「騙案預警」計劃

反詐騙警示及建議會以下列途徑發放：



或



或



3招 提防騙徒假冒「反詐騙協調中心」

1. 中心的短訊發送人名稱為「#ADCC18222」，短訊並不會附有任何連結
2. 中心不會指示受害人轉帳及要求提供銀行理財密碼
3. 如對中心人員身份存疑，可致電
18222熱線查詢

警方亦推出了「防騙視伏App」流動應用程式
協助市民辨識詐騙及網絡陷阱和提升他們的防罪意識



關注我們

香港警務處電子報案中心

<https://crp.police.gov.hk/crp001/>

「防騙易18222」熱線

懷疑受騙
即打 **18222**
www.adcc.gov.hk

「防騙易18222」二十四小時電話諮詢熱線，為市民提供即時諮詢，以便更有效處理懷疑騙案

「反詐騙協調中心」網頁

<https://www.adcc.gov.hk>

Website



小紅書



TikTok



YouTube



關注我們獲取最新防騙資訊

下載及安裝「防騙視伏App」應用程式

<https://cyberdefender.hk/scameter/>

協助公眾辨識詐騙及網絡陷阱，透過輸入有可疑的平台帳戶名稱、銀行帳戶號碼、電話號碼、電郵地址等，以評估詐騙及網絡安全風險



「守網者」一站式網絡資訊平台

<https://cyberdefender.hk>

立即獲取最新網絡安全及防騙資訊

Youtube



Facebook



Website



Instagram

