

# 「安全使用 WhatsApp及社交平台」 講座

鍾麗玲  
個人資料私隱專員

2023年12月8日





# WhatsApp 帳戶遭騎劫及盜用

PCPD



HK

香港個人資料私隱專員公署  
Office of the Privacy Commissioner  
for Personal Data, Hong Kong

即時通訊軟件已成城市人生活必備工具，且載有大量個人資訊，稍一不慎便成為騙徒詐騙的缺口。有騙徒入侵如 WhatsApp、Telegram、Signal 等帳戶，「騎劫」事主帳戶後向其親友下手騙財，有主事的生意夥伴便因此被騙走100萬元人民幣。警方指，近日網上帳戶騎劫案驟升，單是8至9月已錄得1,386宗，九成六涉WhatsApp，總涉案損失達2,820萬元。警方建議市民勿點擊可疑連結，為帳戶設雙重認證鎖，並留意通訊軟件「已連結裝置」情況，若有懷疑先登出；同時可利用警方的「防騙視伏器」搜尋對方戶口、電話或網址是否有可疑。

## 市民被騙100萬元人民幣過程

- 1 騙徒入侵並「騎劫」事主的WhatsApp帳戶。
- 2 騙徒在事主WhatsApp帳戶，選定詐騙目標。
- 3 事主生意朋友被誘騙，轉帳100萬元人民幣至騙徒戶口。

警方指，近年損失最大宗網上帳戶騎劫案涉及一名找換店職員，其WhatsApp帳戶疑被入侵騎劫後，騙徒透過通訊錄向與事主經常有生意往來的朋友發訊息，聲稱當日人民幣兌換率非常可觀，邀對方兌換人民幣；朋友誤以為真，先後兩次共合100萬元人民幣轉帳至騙徒提供的2個內地銀行戶口。事主當日透過微信與該朋友傾談後，才發現WhatsApp被騎劫。

網絡安全及科技罪案調查科網絡安全組高級督察陳智強指，網上帳戶被騎劫早於10年前出現，由最初黑客入侵，至近期常見「釣魚短訊攻擊」和「搜尋器優化中毒」攻擊。「釣魚短訊攻擊」是騙徒發送刻意連結的釣魚短訊，用戶因此進入假網站，假網站套取用戶電話號碼並要求WhatsApp平台向用戶發放轉移代碼，騙徒再向用戶套取轉移代碼，便可騎劫用戶的WhatsApp帳戶。

至於「搜尋器優化中毒攻擊」，騙徒會製作假網頁的登入版面，以WhatsApp作為關鍵字投放廣告，並以贊助方式，讓假網站在搜尋結果中置頂，用戶不小心進入假網頁，將權限二維碼，帳戶便會被入侵。

網絡安全及科技罪案調查科網絡安全組高級督察陳智強指，騙徒騎劫帳戶後，會選擇關係密切但較少溝通的聯絡人，觀察通訊錄談話內容，再以各種口借債或轉帳，並以各種方式隱蔽之間對話，包括將對話封存或即時刪除，令用戶家在鼓裏，直至用戶與該聯絡人透過電話或其他渠道聯絡，才發現帳戶被騎劫。他指，市民其實有方法防範，除WhatsApp啟用雙重認證功能外，使用Android用戶可點擊右上角三點，而iOS用戶則點擊右下角「設定」，就能選擇「已連結裝置」，檢查WhatsApp所有已連結的裝置，如發現有可疑裝置，應即時「登出」，騙徒便會被強制登出。

「防騙視伏App」明年接受市民「報料」

陳智強補充，其中一個最有效的方法，是用去年9月推出的「防騙視伏器」，推出以來累計搜尋次數已逾160萬次，被標記為紅色、橙色及黃色的搜尋結果佔一成半，即與詐騙或網絡安全風險有關的搜尋有超過26萬次，而紅色警告是經證實、非常危險的戶口、電話或詐騙網址。警方透露，「防騙視伏器」資料庫獲銀行界、電信商等約15家公私機構支持，得到不少資訊和情報，並計劃明年第一季在「防騙視伏」App推出「報料」機制，讓市民收到古怪來電後可透過App舉報，進一步豐富「內容」。警方在上月中至本月上旬向595名「防騙視伏器」用戶調查，所有受訪者均表示自己會接觸不同類型的網絡詐騙陷阱，其中42.7%認為自己尚未具備足夠能力識別網絡詐騙陷阱。他強調，騙徒極目標是錢，駭客傳教能提高市民警覺和警覺性，轉帳前三思。

漁翁撒網找目標 受害人陷假投資平台失60萬

除騎劫戶口，騙徒亦會漁翁撒網尋找詐騙目標，化名林先生的受害人分享經歷，指3月在Signal收到一名自稱在加密貨幣交易所工作、名叫珊的陌生女子訊息，稱原欲聯絡朋友，卻誤向林先生發訊息，雙方交談後言談甚歡，林應邀助辦操作2個虛假帳戶，並曾賺取3.5萬港元。林其後聽從對方指示開設戶口，實行「有錢買賣」，在指定平台開戶，儲值10萬USDT(泰達幣)，短時間內賺取3萬USDT獎勵。林先生指，珊之後以各種藉口要求他投入更多錢，才能提取本利。他坦言，曾透過提供安全檢查網站免費服務的ScamAdviser，警方「防騙視伏器」評估珊提供的交易平台網址，收款帳戶和WhatsApp客服號碼，雖然結果均顯示為「與詐騙相關」的紅色警告，但他最終仍相信珊「不是騙徒」的各種「解釋」，繼續按照對方指示再3次投入資金，總共約27萬港元，直至交易平台關閉，才確定被騙，共損失60萬元。

心理學家：睇準受害人怕一切付諸流水

警察臨床心理學家馮浩整分析林先生個案，指騙徒會令受害人以為得到難得機會，如投資秘訣，錯失機會「對唔住自己」，被帶到不熟悉的領域後，騙徒又扮演專家，受害者想「依靠」，更容易相信騙徒。他指，在受害人投入很多資源、金錢後，即使有懷疑仍不會接受逃騙，否則一切付諸流水；此時，騙徒只須講出預早想好的回答，受害人就會忽視辯解的含稱，繼續相信騙徒，陷得更深。

即時通訊軟件帳戶騎劫案驟升

九成六涉WhatsApp  
慎防釣魚短訊  
防搜尋器攻擊

防範WhatsApp被騎劫兩部曲

可加入「已連結裝置」或「帳戶」

「已連結裝置」可看到已連結裝置數量

加入「帳戶」設定「雙重認證」

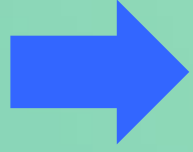
AM730 Media Limited

香港灣仔皇后大道中160號廣生行大廈10樓

JJ printing limited

將軍澳康翠閣七號將軍澳工業邨

騙徒騎劫受害人的WhatsApp 帳戶



冒認受害人向其親友發送詐騙訊息騙取金錢或個人資料

WhatsApp 報料熱線 91999933

朋友 防騙系列

收騙徒加料訊息

你網上銀行，轉數快有無2萬，幫我過下數，聽日過翻比你

劇科發展協會主席 陳迪源

專家教一招斬續

事主 與朋友對話

WhatsApp 騎劫新招 事主懵然不知

被駭帳戶 瘋狂問朋友借錢

星島 申訴王

有冇你裝成

有無 constance 19

gold

kelly 25

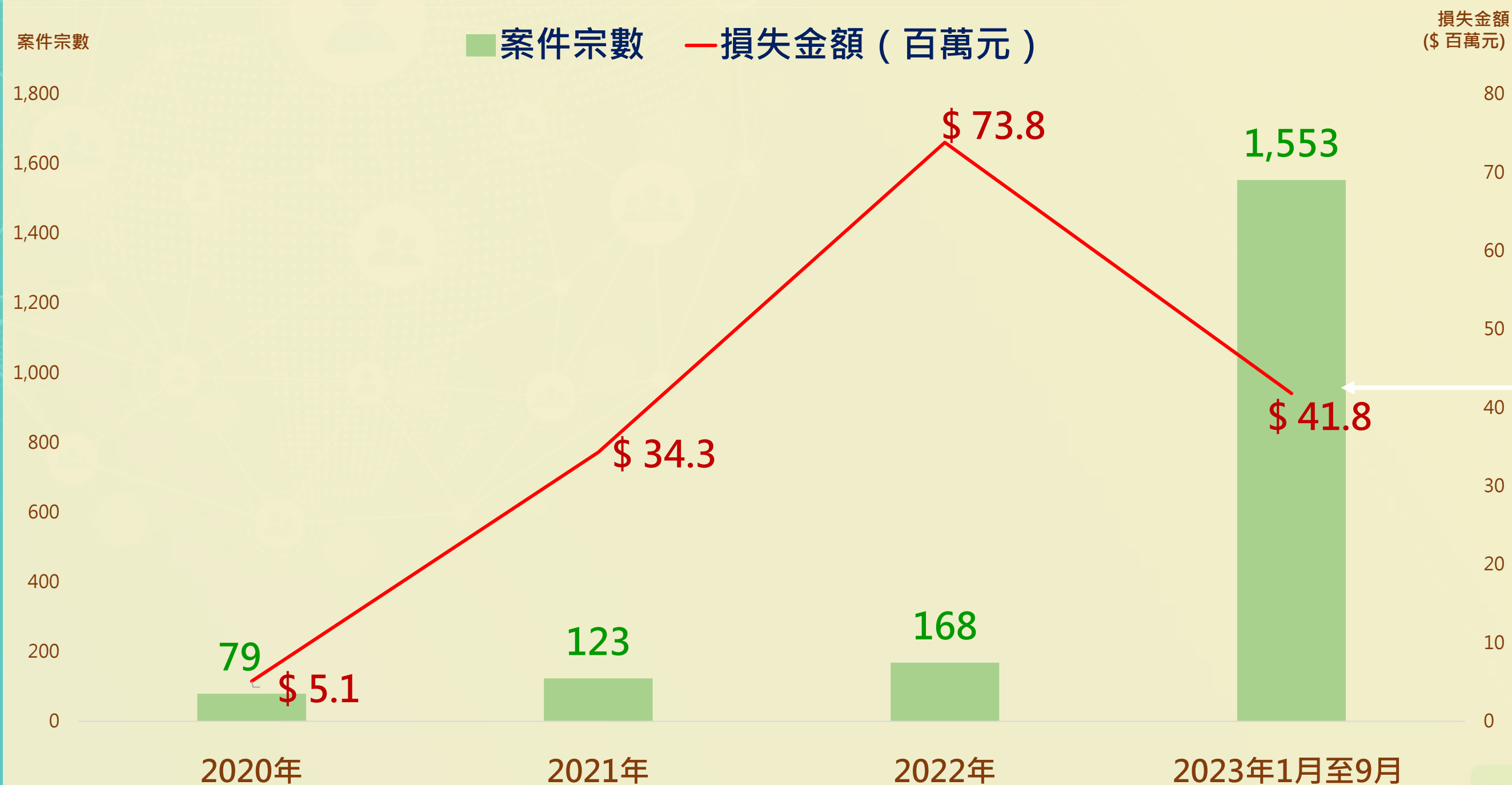
已離開

你網上銀行，轉數快有無2萬，幫我過下數，聽日過翻比你





# 涉及「網上戶口盜用\*」的 案件宗數及損失金額

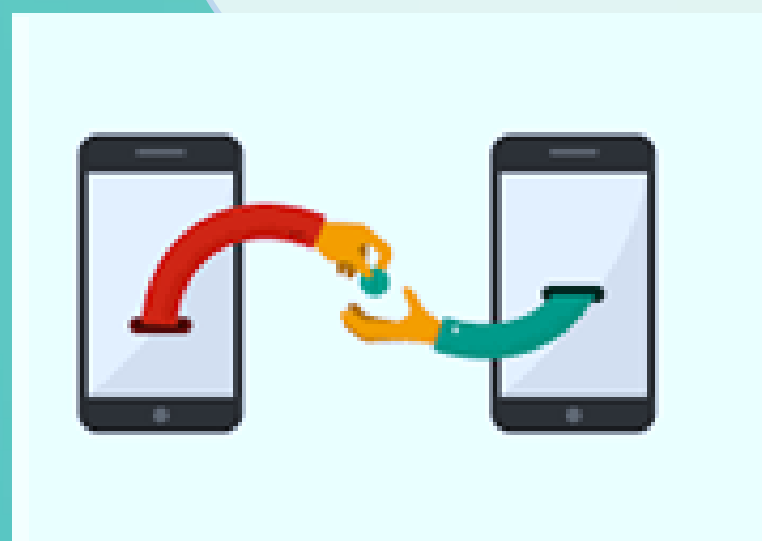


其中1,334宗案件及  
2,800萬損失金額  
涉及即時通訊軟件  
帳戶騎劫

\*「網上戶口盜用」包括透過社交媒體、網上支付工具、電郵等帳戶盜用案件。  
鑒於近期即時通訊軟件帳戶騎劫騙案明顯增加，警方自2023年8月起將相關騙案數字  
納入「網上戶口盜用」類別作統計。

# 與WhatsApp騙案有關的常見查詢

- **市民**表示其WhatsApp帳戶遭騎劫，騙徒繼而盜用他們的帳戶假冒有關市民，**向通訊錄的聯絡人發送訊息騙取金錢**。有關市民向私隱專員公署查詢如何應對有關情況。
- **機構**表示有騙徒騎劫其帳戶，並**向他們的服務使用者或客戶發出訊息，要求他們付款**。機構查詢是否須向私隱專員公署作出資料外洩事故通報。





# 騎劫WhatsApp帳戶的常見手法

## 釣魚訊息

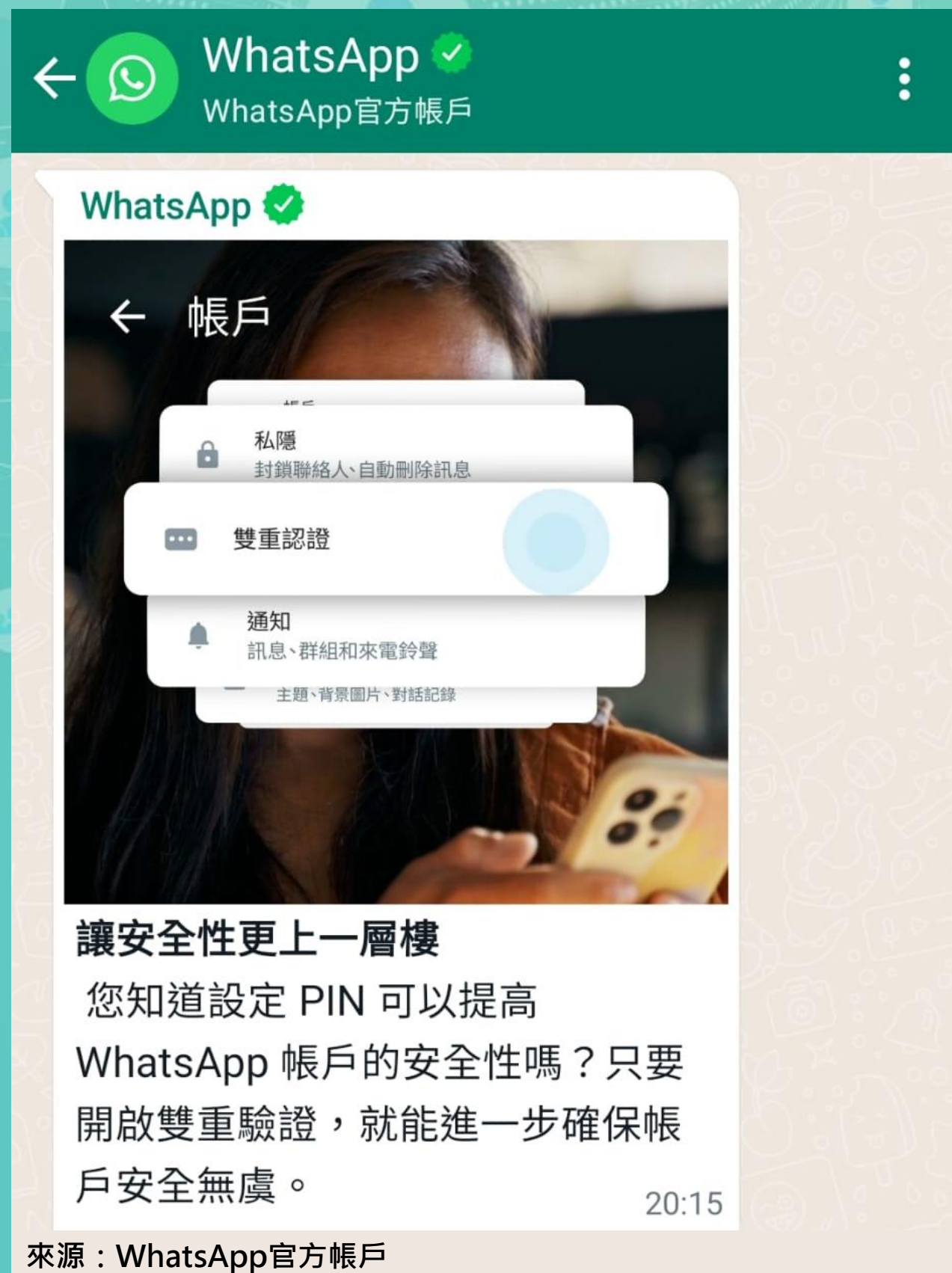
騙徒假扮受害人的親友發出  
**WhatsApp** 訊息，誘騙受害人轉發其WhatsApp帳戶的  
**驗證碼**，以登入其帳戶



# 騎劫WhatsApp帳戶的常見手法

## 假冒短訊

假冒WhatsApp發出短訊，誘騙受害人按下連結至**假網頁**，騙取其**電話號碼**及WhatsApp帳戶**驗證碼**，以登入其帳戶





# 騎劫WhatsApp帳戶的常見手法

無收釣魚短訊 無印象泄露驗證碼  
**WhatsApp帳戶都被騎劫?**  
好可能因為去咗假網站 ↓↓

The screenshot shows a search engine interface with the word 'Search' at the top. Below it is a search bar containing 'whatsapp'. Three search results are listed:

- 贊助**  
waa.whaitas.cyou (假)  
WhatsApp官方 - WhatsApp中文網  
最新高 端 加密让 您的个人消息和通话更有安全保障。 直接从电脑发送和接收WhatsApp 消息。
- 贊助**  
waa9.edllkikk.com (假)  
WhatsApp电脑版 - WhatsApp官网  
可助您触达全球客户, 规模化打造引人入胜的体验, 提高业务销量以及建立客户关系。 用文字, 也能肆意展现自我, 发布动态来分享每日点滴。
- https://www.whatsapp.com (真)  
WhatsApp | 安全、可靠的免費私人訊息和通話功能  
使用WhatsApp Messenger 與親朋好友保持聯繫。WhatsApp 提供簡單安全又可...和通話服務, 並且在世界各地的手機上皆可免費下載使用。

來源：守網者

## 假冒網站

於搜尋網站放置**假冒的WhatsApp網站**，誘騙受害人輸入其**電話號碼**及WhatsApp帳戶**驗證碼**，或掃描二維碼，以登入其帳戶





# 保障WhatsApp帳戶的措施

啟用  
WhatsApp  
雙重認證功能

定期在  
WhatsApp設定中檢查已連結裝置

切勿向他人透露  
任何密碼或  
驗證碼

小心誤按虛假的WhatsApp  
網頁版

切勿從非官方  
渠道下載及使用WhatsApp  
應用程式

一旦收到可疑  
訊息，先確認  
發送者的身分

切勿隨意打開  
連結或披露  
個人資料





# 復原遭盜用WhatsApp帳戶

1. 以你的手機號碼登入 WhatsApp



2. 輸入你於SMS短訊收到的 6 位數  
驗證碼來驗證手機號碼



3. 當你輸入驗證碼後，  
盜用你的帳戶的人便會被自動登出



- 如需輸入**雙重認證驗證碼**，而你不知道此驗證碼，那可能是盜用你的帳戶的人已啟用雙重認證功能
- 若你沒有此驗證碼，**等待7日後**便能登入你的帳戶





# 小心使用社交媒體平台



私隱專員公署檢視了香港十大最常使用的社交媒體的私隱功能、私隱政策及私隱版面易用性，並於去年發表報告

- Facebook
- Facebook Messenger
- Instagram
- LINE
- LinkedIn
- Skype
- Twitter
- WeChat
- WhatsApp
- YouTube





## 查閱私隱政策

### 檢視結果重點（只列部份）

- 被檢視的社交媒體均會收集用戶的**位置資料**
- 部分社交媒體預設公開用戶的**年齡、位置、電郵地址或電話號碼等個人資料**
- 大部分被檢視的社交媒體均會儲存用戶的**信用卡資料**
- 所有社交媒體均在私隱政策中列出會將用戶個人資料**轉移**  
**到其附屬公司**





# 實用建議 - 在註冊社交平台帳戶時

## 減少提供 個人資料

- 如非必要，切勿提供**敏感個人資料**。例如，詳細地址和完整的出生日期
- 如須提供電郵地址，應開設一個**專用的電郵帳戶**以作登記



## 保障 帳戶安全

- 設定**高強度**、**獨特**的密碼
- 如社交媒體平台有提供**多重身份認證**，應採用有關功能





# 實用建議 - 在使用社交媒體時

## 調整私隱 設定



- **資訊的公開程度**，例如個人經歷、個人聯繫、聯絡資料及帖文等
- 即時通訊軟件上的**個人頭像**和**狀態**
- **平台可獲取的權限**，例如臉容識別、定位追蹤及網上跨平台追蹤等
- 容許其他用戶「**標註**」或「**提及**」你
- 容許其他人利用你的電郵地址或電話號碼對你**作出搜索**
- **第三方應用程式查閱**你的社交媒體個人檔案的權限





# 實用建議 - 在使用社交媒體時

## 分享及 發送資訊

- 分享或發送任何資訊前**應三思**，按鍵的一刻，資料即成為數碼足跡
- 考慮所分享的資訊的**公開程度**（例如只限朋友還是向所有用戶公開）
- 在標註他人或分享他人的資訊時，應先獲得當事人的**同意**
- 定期檢視過往帖文，**刪除**不再想分享的資料
- 向平台「**舉報**」有關於你私人、敏感或不當資訊的內容







## 指引資料

香港個人資料私隱專員公署  
Office of the Privacy Commissioner  
for Personal Data, Hong Kong

### 保障個人資料私隱— 使用社交媒體及即時通訊软件的指引

#### 關於本指引

社交媒體及即時通訊軟件在香港被廣泛使用。然而，使用社交媒體及即時通訊軟件會為用戶的個人資料私隱帶來不容忽視的風險。本指引旨在指出這些風險，並提供減低風險的實用建議。

#### 社交媒體、即時通訊軟件及其服務

社交媒體及即時通訊軟件涵蓋多種網上平台和服務，這些平台和服務的設立目的是供用戶交流以及製作和分享内容。本指引統稱兩者為「社交媒體」。

雖然大部份社交媒體平台都不收取任何費用，但不等於有關服務是「免費」，皆因用戶的個人資料會被收集和分享。用戶在平台進行活動（例如閱讀帖文或對帖文按讚）或使用其服務（例如發送訊息）時，這些資料通常都會被收集作個性分析之用。這類用戶活動所產生的大量資料，有時甚至在用戶不知情下被採集，會被社交媒體平台用於廣告活動或再分享而從中獲利。

#### 與使用社交媒體及即時通訊軟件相關的個人資料私隱風險

- 私隱受損
  - 若用戶在社交媒體過度分享資訊，便會在不知不覺間透露比預期中更多的個人資料。
  - 幾乎所有在社交媒體分享的事情都會留下永久的數碼足跡，並且難以從網絡中刪除。
  - 發送至個別用戶的即時訊息，即使已被加密，仍可由接收者轉發或廣泛地分享。



下載本刊物



香港個人資料私隱專員公署  
Office of the Privacy Commissioner  
for Personal Data, Hong Kong

## 個人資料咪亂俾 踢走騙徒靠晒你

Don't Hand Over Your Personal Data  
Beware of Fraudsters

個人資料防騙熱線  
Personal Data Fraud Prevention Hotline  
☎ 3423 6611

防騙熱線：  
3423 6611

資料及活動 | 執法報告 | 常問問題 | 審查及執法 | 「起底」罪行 | 數據安全 新! | 防騙貼士 新! | 投訴 | 教育及培訓 | 資源中心 |

香港個人資料私隱專員公署  
Office of the Privacy Commissioner  
for Personal Data, Hong Kong

關鍵字搜尋

RSS A A

#### 防騙貼士



私隱專員提提大家  
8招防騙貼士

- 1 「+852」字頭的來電有可能是詐騙電話
- 2 不要輕信陌生來電、電郵或短訊內容
- 3 聯絡相關機構查證
- 4 切勿隨意披露任何個人資料
- 5 切勿開啟可疑電郵或短訊內的連結或附件
- 6 留意帳戶登入的紀錄
- 7 不時更換帳戶的密碼
- 8 提醒親友小心詐騙

個人資料防騙熱線  
3423 6611

香港個人資料私隱專員公署  
Office of the Privacy Commissioner  
for Personal Data, Hong Kong





謝謝！

*Thank you!*

