「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

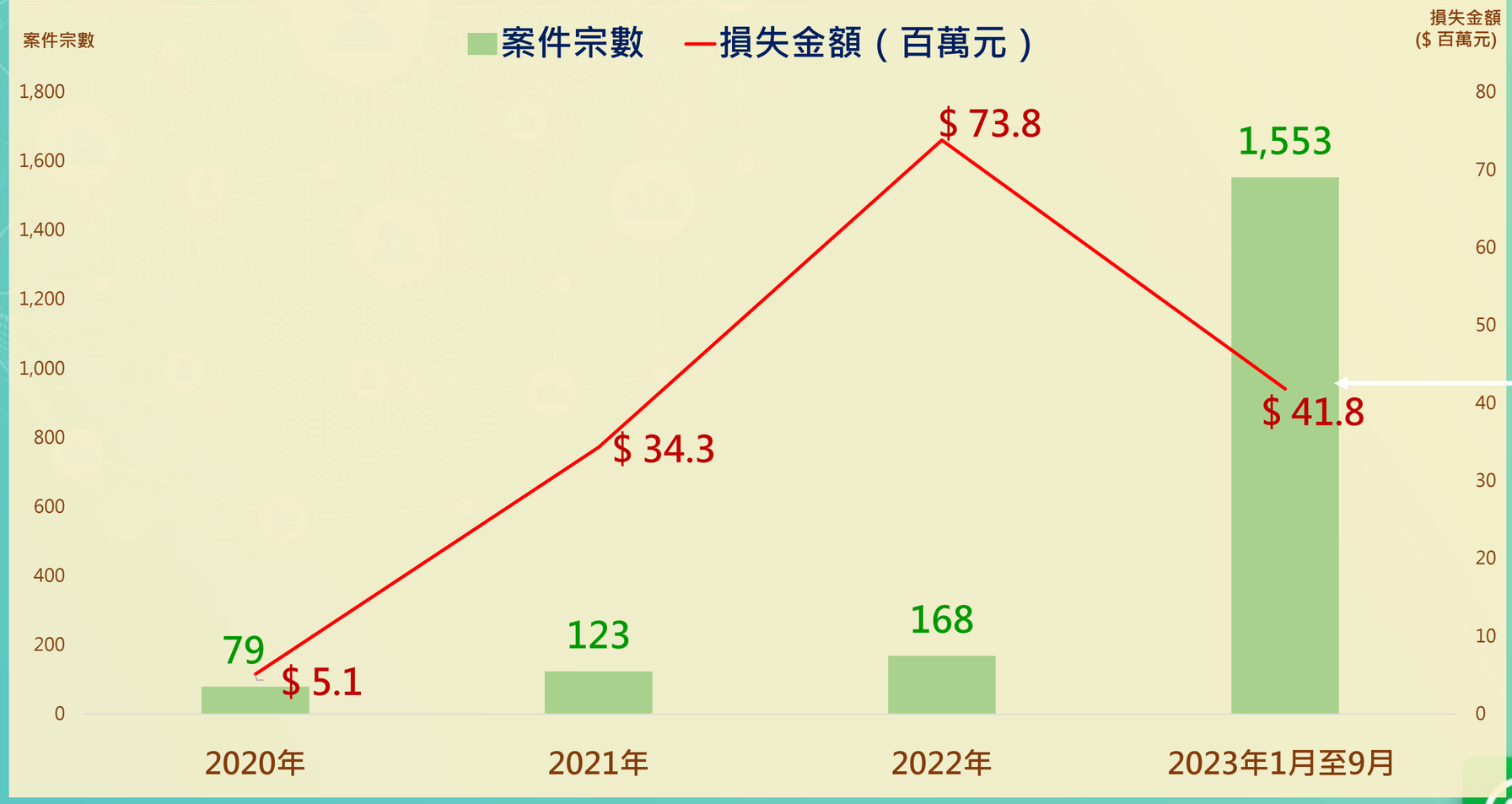
香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

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**

涉及「網上戶口盜用*」的案件宗數及損失金額

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



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

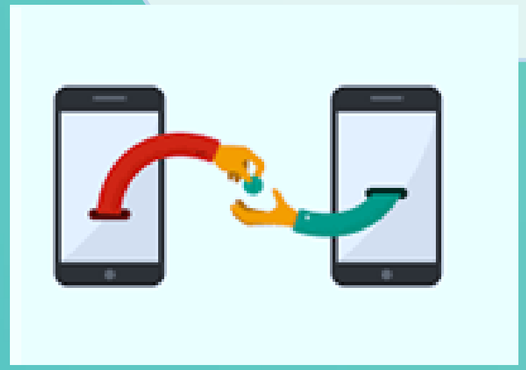
*「網上戶口盜用」包括透過社交媒體、網上支付工具、電郵等帳戶盜用案件。
鑒於近期即時通訊軟件帳戶騎劫騙案明顯增加，警方自2023年8月起將相關騙案數字納入「網上戶口盜用」類別作統計。

來源：立法會

與WhatsApp騙案有關的常見查詢

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

- **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

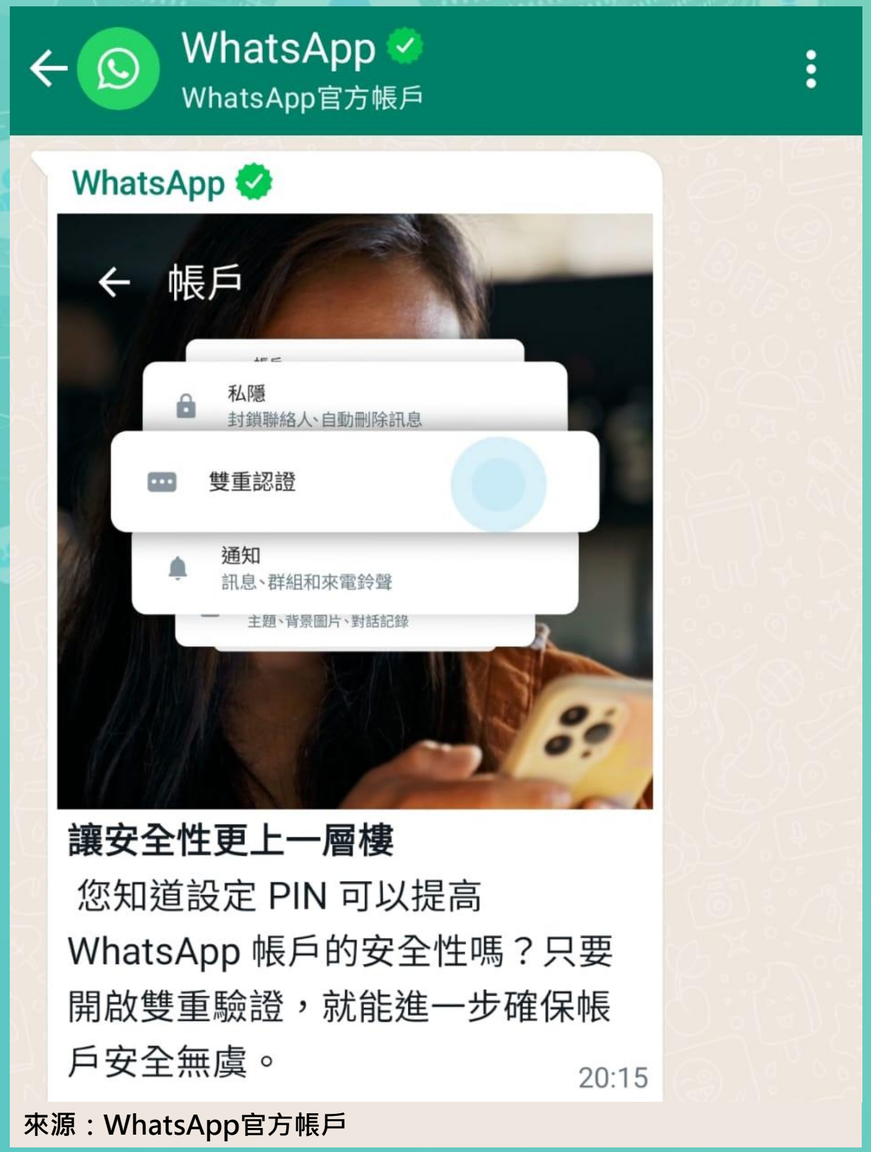
香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

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

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



來源：WhatsApp官方帳戶

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

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

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**，或掃瞄二維碼，以登入其帳戶

保障WhatsApp帳戶的措施

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

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

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

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

NOTE

- 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

來源：WhatsApp

小心使用社交媒體平台

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

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*

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

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

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

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

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

調整私隱設定

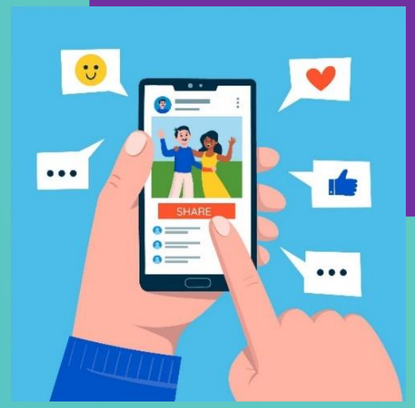
- **資訊的公開程度**，例如個人經歷、個人聯繫、聯絡資料及帖文等
- 即時通訊軟件上的**個人頭像**和**狀態**
- **平台可獲取的權限**，例如臉容識別、定位追蹤及網上跨平台追蹤等
- 容許其他用戶「**標註**」或「**提及**」你
- 容許其他人利用你的電郵地址或電話號碼對你**作出搜索**
- **第三方應用程式查閱**你的社交媒體個人檔案的權限

實用建議 - 在使用社交媒體時

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

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



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

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

PCPD.org.hk

保障個人資料私隱—
使用社交媒體及即時通訊軟件的指引

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大家
以及製作和分享內容。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
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（
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
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

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
  - 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
  - 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
    三者。

下載本刊物

1

保障個人資料私隱—使用社交媒體及即時通訊軟件的指引　2021年4月

防騙熱線：
3423 6611

PCPD
H K

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!