

今年首7個月警方錄得1,993宗騎劫WhatsApp賬戶的騙案，按年急增1,254宗，升幅169.7%，損失金額1.463億元。騙徒透過不同途徑發釣魚短訊，假冒WhatsApp官方信息誘用戶進入假網站，從而騎劫其賬戶，以及搜尋賬戶內電話簿和分析聊天紀錄，再冒充親友、同事、上司或商業夥伴詐財，當中冒充親友的騙案佔86%，但冒充上司或商業夥伴往往能獲巨大騙款，今年損失最嚴重的WhatsApp騙案涉及一名財務經理，騙徒冒充其「上司」騙取1,220萬元，其次是一名經商的兒子跟從「父親」指示被騙逾千萬元。

● 香港文匯報記者 曾立本



● 警方今年首7個月錄得1,993宗騎劫WhatsApp賬戶的騙案，較去年同期急增169.7%。圖為市民外出使用手機。

警方網絡安全及科技罪案調查科警司許綺惠表示，今年首7個月科技罪案宗數及損失錄得雙位數跌幅，但即時通訊軟件賬戶騎劫案逆市飆升，共錄得2,020宗，按年增1,255宗，涉款約1.504億元，按年減少約4,140萬元。當中涉及WhatsApp騙案達1,993宗（佔通訊軟件騙案99%）。

許綺惠說，WhatsApp賬戶被騎劫的真正風險，是騙徒可以取得WhatsApp內電話簿及聯絡人，從而聯絡受害人親友或工作夥伴進行詐騙，在1,993宗WhatsApp賬戶騎劫案中，騙徒主要利用受害人親友關係犯案，冒充親人佔806宗、朋友佔785宗，合共佔86%。

騙徒騎劫WhatsApp賬戶設騙局有三個階段。首先，冒充WhatsApp官方發出釣魚短訊，以催促性語氣製造緊迫感，要求用戶立即點擊連結。亦有騙徒透過陌生WhatsApp號碼直接聯絡受害人。另外騙徒利用「搜尋引擎投毒」（Search Engine Poisoning），包裝成廣告或贊助推薦內容，令假冒的WhatsApp網站出現在搜尋結果（甚至會置頂），受害人一不留神便會登錄有關網頁，之後騙徒會要求事主輸入手機號碼、驗證碼、8位數配對碼或掃描QR Code，以完成裝置連結程序，從而騎劫該賬戶。當騙徒取得賬戶控制權後，會利用事主原有的通訊錄及信任關係，對其親友、同事或商業夥伴發出付款要求。

偽經紀催落訂 上車客失逾百萬

今年3月一名32歲男子初次置業，簽訂臨時買賣合約及支付「細訂」，其間透過WhatsApp與地產經紀及律師聯絡，至月中收到WhatsApp的釣魚短訊，並按要求點擊連結及進行「賬戶驗證」，被騙徒騎劫其WhatsApp賬戶，並搜查其聊天紀錄資料，發現受害人正在辦理買樓手續。騙徒遂利用兩個不同電話號碼及偷來的頭像，冒充地產經紀和律師與受害人商討餘下的手續，成功騙取受害人117萬元「大訂」。

假父親要轉錢 商人被呃逾千萬元

其中，一名商人因與父親有很多生意往來，父子之間不時有金錢轉賬。今年7月，案中父親的賬戶遭騎劫，騙徒遂利用AI生成語音錄音，冒充父親對話的語音信息，以朋友、供應商或商業夥伴急需資金周轉等理由，要求兒子轉賬，事主不以為意，多次轉賬，最終損失逾千萬元。

另外，一間投資公司的財務經理，今年1月騙徒冒充其上司透過WhatsApp發短訊，聲稱有一個機密投資項目，要求安排付款。由於受害人見有關信息是由上司賬戶發出，遂按指示多次轉賬到不同銀行戶口，合共1,220萬元。直至公司發現流動資金突然減少逾千萬元，才令受害人起疑，轉用WeChat向上司發短訊了解，始發覺上司從來沒作出轉賬指示，懷疑其WhatsApp賬戶被騙徒騎劫設局行騙。

警方網絡安全及科技罪案調查科總督察黃長興提醒市民，凡涉及「驗證碼」、「掃描二維碼」或「重新驗證賬號」，「一定要停一停、諗一諗」；收到透過WhatsApp要求轉賬或付款短訊，應使用另一個獨立管道審核對方身份，主動提問只有雙方知道、無法從過往WhatsApp對話中找到的數據；轉賬前仔細檢查收款戶口。



● 觀塘警區重案組第一隊督察黃凱瑩展示檢獲的證物。香港文匯報記者林兆崙攝

首7個月騎劫WhatsApp騙案急升169.7% 掠財近1.5億

近九成騙徒扮親友 假上司偽夥伴呢巨款



資料來源：警方網絡安全及科技罪案調查科

收到聲稱WhatsApp賬戶被限制、停用或需要重新驗證的信息，切勿急於點擊連結，亦不要提供驗證碼、8位數配對碼或掃描不明二維碼。

如親友、上司、同事或商業夥伴突然透過WhatsApp要求轉賬或付款，應使用另一個獨立渠道核實身份。

核實對方身份時，可詢問只有雙方才知道、而且不容易從過往WhatsApp對話中找到的資料。

轉賬前應核對收款戶口，如突然要求轉往陌生第三方戶口、轉數快或電子錢包，應提高警覺並再次核實。

定期檢查WhatsApp的「已連結裝置」（Linked Devices），如發現陌生裝置，應立即登出。

減少在公開社交平台披露多個人、家庭、工作及聲音資料。

如有懷疑，可使用警方「防騙視伏器」或致電「防騙易」熱線18222查詢。

整理：香港文匯報記者 曾立本



騎劫WhatsApp賬戶三部曲

1 冒充WhatsApp官方發出釣魚短訊，聲稱賬戶「違反服務條例」、「身份驗證失效」、「被投訴」或「即將被停用」，並設定短時間限期，製造緊迫感，要求用戶立即點擊連結。另外，騙徒亦會利用「搜尋引擎投毒」（Search Engine Poisoning），包裝成廣告或贊助推薦內容，令假冒的WhatsApp網站出現在搜尋結果（甚至會置頂），受害人一不留神便會登錄有關網頁。

2 受害人進入假冒的WhatsApp網站後，被要求輸入手機號碼、WhatsApp驗證碼、8位數配對碼或掃描QR Code，以完成裝置連結程序；受害人以為正在進行賬戶驗證，但其實騙徒已在後台竊取資料，用另一部裝置登入其WhatsApp賬戶。

3 騙徒取得賬戶控制權後，會利用受害人原有的通訊錄及信任關係行騙，並可能查看可取得的對話內容，了解受害人與親友、同事或商業夥伴的溝通模式及金錢往來。當選定目標後，騙徒會模仿事主語氣，向其親友、同事等發出付款要求。

登入手機及WhatsApp 專家倡雙重驗證

專家之言

Meta亞太區產品公共政策總經理蔡錦文表示，面對騙徒犯案手法愈趨精密，業界、執法部門及社會各界必須攜手合作共同應對。WhatsApp分別從設計層面預防傷害、增強用戶控制功能、偵測潛在濫用行為、與外部專家及執法機構合作等，全方位保障用戶安全。

蔡錦文說，用戶接到未知來電時，除會顯示國家或地區代碼外，還會提示來電來自其他國家或地區、對方不在通訊錄中，以及用戶與對方沒有任何共同群組或對話紀錄。除非用戶主動參與互動，否則不允許點擊任何連結，也會阻止可疑連結出現在WhatsApp聊天中。他呼籲用戶使用雙重驗證，通過面部掃描或指紋進入手機設備和WhatsApp賬戶。

警方網絡安全及科技罪案調查科警司許綺惠提醒，市民不要只聚焦WhatsApp保護，不同即時通訊軟件或社交平台用戶，也應該定期檢查有否啟動相關私人保障措施或安全設定。但設定技術防護只是第一重保護，最重要是市民必須有防範意識。警方為提升市民防騙意識，持續推行宣傳及公眾教育，例如舉辦防騙講座。

警：假冒訊息轉交平台移除

此外，警方與業界保持緊密合作，將數以萬計假冒WhatsApp短訊等資料，提交Meta及其他平台移除，同時透過即時交換情報，掌握最新詐騙手法及保安功能，以協助市民防騙。

警方不斷加強線上線下巡邏，去年至今共破獲5宗涉及偽基站案件，其中上月30日在將軍澳截獲一部私家車，發現正在運行的偽基站設備，相信有人企圖利用偽基站干擾附近手機信號，令手機降至2G網絡，繼而繞過電訊商發送假冒WhatsApp的詐騙短訊，司機及車主被捕，相信他們已發送逾6,000條詐騙短訊，涉及至少16宗案件，涉款約30萬元。

● 香港文匯報記者 曾立本

警搗「貓池」電騙中心 拘兩男涉扮假客服呢60萬

香港文匯報訊（記者 蕭景源）警方商業罪案調查科早前根據線報及調查，前日搜查荃灣區一酒店房間，搗破一個利用俗稱「貓池」的電話數據機收發大量電話及釣魚短訊的電話騙案操控中心，檢獲53張屬於他人實名登記的流動電話卡和小量「冰」毒，以涉嫌串謀詐騙及管有危險藥物罪拘捕兩名男子。初步相信他們與8月下旬至少5宗假冒客服的電話騙案有關，涉款近60萬元。

被捕兩人分別26歲及38歲，其中一人有三合會背景，警方相信已瓦解一個由三合會控制的電話騙案操控中心。調查顯示，他們曾向不同人士購買大量實名登記的電話卡，再以「貓池」致電受害人，向他們訛稱是保險公司或支付平台，指受害人已開通保險服務並遲交款項，若不取消會被扣款。受害人情急下遂根據騙徒指示，操作自己的網上

銀行戶口，在轉賬界面上，按騙徒指示輸入一些銀行戶口或轉數快號碼作為收款人，再輸入一些聲稱是驗證碼的數字至轉賬銀碼的位置進行操作。受害人其後發現相關款項在自己戶口被轉走始發現受騙，因而報警求助。

警方相信，涉案團夥曾向市民發送短訊，聲稱是網購平台或速遞公司，訛稱受害人的派遞失敗，並提供所謂的客服熱線以供查詢。當受害人致電熱線時，騙徒會以不同藉口要求轉賬至指定的銀行戶口，繼而失去聯絡，令受害人蒙受損失。

租酒店房作電騙中心 檢懷疑「冰」毒

觀塘警區重案組第一隊督察黃凱瑩表示，警方經調查後，發現涉案兩人租用荃灣區一酒店房間作為電話騙案的操控中心。警員上周五（28日）掩至酒店房拘

捕他們，同時檢獲一部「貓池」機、3部手提電話、兩部電腦及53張屬於他人登記的電話卡，另有5包共重約1克懷疑「冰」毒及一個懷疑毒品吸食工具。

據了解，騙徒在上址酒店短租房間用作電騙操控中心。案中單一損失最大金額約38萬元，受害者是一名退休人士，他因收到騙徒的短訊，表示派遞失敗，要求致電客服查詢，繼而按騙徒指示輸入所謂的驗證碼數字至轉賬銀碼的位置操作，結果被騙。

警方再次提醒廣大市民，收到任何來歷不明的電話，尤其是當對方要求索取金錢、銀行戶口資料及密碼時，要加倍小心；如有疑問，應直接透過官方渠道聯絡相關機構查詢。同時，市民切勿向他人出售自己實名登記的電話卡。若有關電話卡被人利用作詐騙或其他不法用途，出售或借出這些電話卡的人士，有機會要負上刑事責任。