WhatsApp賬戶遭騎劫 黑客扮你騙親友

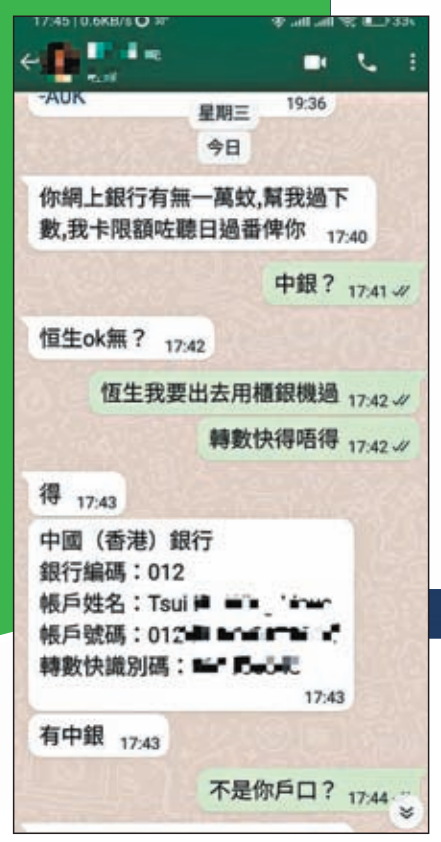
受害人：阿女問起方知情 5社福機構學校中招洩近900人私隱

網上騙

案層出不窮，香港近日出現多宗手機即時通訊程式遭黑客入侵並假冒用戶向親友借錢事件。香港私隱專員公署5日透露，過去一個月已接獲5間社福機構及學校資料外洩事故通報，指用作與受助人、學生或家長通訊的即時通訊軟件WhatsApp賬戶被「騎劫」，假冒受害機構向通訊錄的聯絡人發送騙取金錢訊息，涉及近900名受助人、學生、家長或職員的姓名及手提電話號碼等個人資料。有WhatsApp用戶亦向香港文匯報表示，有騙徒冒認他向朋友及其女兒借錢，幸由於騙徒提供的銀行賬戶並非其姓名，其朋友才未上當。另一名Telegram用戶亦被騙徒冒充他借錢，同一日亦有人假扮其親人意圖向他行騙。

◆香港文匯報記者 劉明

▲5日Google搜尋結果仍可見僞冒WhatsApp網站。



◀朋友向阿Paul展示騙徒向其借錢的對話，因提供的並非阿Paul銀行戶口而令他懷疑，幸而未有受騙。

◆騙徒在蝌蚪的Telegram賬戶內冒充他，向其朋友借錢，幸朋友有懷疑而拒絕。

私隱專員鍾麗玲接受電台訪問時透露，在約900名受影響人士中，有個案或涉及住址和銀行資料外洩，但仍要調查有關情況，相關機構及學校已根據私隱專員公署建議通知受影響人士。

她指出，由去年至今年8月，公署並未接到同類通報，上月卻錄得5宗通報，反映WhatsApp賬戶遭「騎劫」明顯增加，但上述個案應屬隨機「騎劫」行為，而非針對有關機構或學校。

假網站或扮親友 騙取驗證碼

公署解釋，WhatsApp賬戶騎劫一般是指假冒受害人親友發出WhatsApp訊息，要求受害人轉發其賬戶驗證碼，或透過假冒WhatsApp網站騙取受害人電話號碼和賬戶驗證碼，以登入賬戶冒充受害人。鍾麗玲坦言，市民未必得悉自己資料外洩，部分人忽視電話號碼外洩的嚴重性，若以電話號碼作為不同賬戶的密碼，被盜用機會就會增加。

有用戶已「雙重認證」一樣中招

WhatsApp用戶阿Paul 5日在接受香港文匯報訪問時表示，自己一向已十分小心保障個人私隱，除早已啟用WhatsApp雙重認證功能外，絕不會在賬戶內透露個人資料，亦從不點擊任何連結，但仍然「中招」，「唯一解釋是我用WhatsApp網上版，因工作需要會利用WhatsApp傳送檔案，有可能下載了假網站，但仍可在假WhatsApp網站傳送資料。有騙徒冒充我向他人借錢，就屏蔽了我，令我不知遭人冒認。」

他表示，該騙徒上月25日在其賬戶冒充他向朋友借1萬元，訛稱銀行卡因限額問題未能過數，翌日會歸還款項，但騙徒所提供的銀行戶口用戶姓徐，亦非其姓名，故引起其朋友懷疑，致電向他查詢，他才知賬戶遭「騎劫」，其朋友亦未有損失。

同時，該騙徒還向他的女兒傳送同一訊息，其女兒卻未有懷疑，「已經想住過數給我，但打來問入落騙徒提供的戶口，還是用『轉數快』過錢，我先知原來最少已有兩人收到騙徒訊息，女兒亦因此未有損失。」

阿Paul其後到警署報案，但有警員表示由於沒有人遭金錢損失，所以只為其備案，「其實騙徒的訊息有銀行戶口同姓名，但警方話好多戶口都是非法得來，要有金錢損失先能夠行動。」

他暫已透過WhatsApp通知所有親友有關事件，着他們切勿受騙，同時會聯絡各親友有否蒙受損失而未有揚聲。

TG有用戶被入侵 盜名借錢

除WhatsApp賬戶，Telegram用戶蝌蚪亦向香港文匯報透露其賬戶遭入侵。4日，有人冒充他在賬戶內聲稱應急，向朋友借3,800元（港元，下同）過數，還稱晚上會在櫃員機入錢還給對方，但其朋友知他不會如此借錢，有懷疑故斷言拒絕。

同一日，他胞妹的Telegram賬戶也被「騎劫」，並向他借3,500元，他同樣感到懷疑以戶口沒有錢打發對方，但騙徒死纏爛打要其幫忙，當中一句：「阿姨講話你不相信？」令他更肯定對方是詐騙，「Telegram用戶是我妹妹，但對方自稱阿姨，所以一定是假。」

對自己的Telegram賬戶被入侵，他表示不知原因，「只是早前收到Telegram訊息話我好耐冇用，叫我更新賬戶，但不知是不是騙徒騙我。」與WhatsApp不同，Telegram未有屏蔽冒騙訊息，他當晚看到賬戶內騙徒向朋友借錢的對話，才知被入侵，立即致電朋友說明情況，亦在WhatsApp通知所有親友有關事件，着他們小心受騙。

僞冒網頁版WhatsApp 被騙密碼即長期「寄生」

專家之言

香港近日湧現多宗利用WhatsApp行騙的案件，有騙徒盜取賬號後，冒充賬號主人的身份，向其親友借錢或索取禮物卡，涉及金額由幾百至逾萬元（港元，下同）不等。香港資訊科技商會榮譽會長方保僑向香港文匯報表示，騙徒主要透過僞造虛假網頁版WhatsApp頁面，或者使用虛假官方賬號發送釣魚連結，誘騙賬號主人提供一次性密碼後，「騎劫」賬號。市民搜查網頁版WhatsApp頁面時，要留意網址有否破綻（如串錯字等），點擊連結時要特別小心。

香港文匯報記者嘗試在Google搜尋「WhatsApp網頁版」，結果發現前列位置均是假冒網站。在點擊連結後，會進入與官方相似的假冒界面，要求用戶掃描QR Code登入。但和「正版」不同的是，頁面文字均以簡體字顯示，域名亦與官方不同。記者稍晚再次在Google輸入關鍵字進行搜尋，發現部分假冒網站已經消失，但不排除騙徒其後再重新製作假網站。

方保僑表示，WhatsApp騙案存在已久，但「騎劫」賬號的手法卻不時更新。近期多發的個案主要涉及虛假的網頁版WhatsApp，騙徒用此手法盜取賬號，然後冒認賬號主人向其好友或群組索要錢財。「有時候用户登陸Web版本WhatsApp，不是透過官方網站，而是用Google搜查，而Google的前兩個廣告連接有機會是假網站，用户掃碼登陸後，騙徒在另一端已經能夠監察住對話，隨時向群組裏面的朋友埋手。」他形容，有些騙案手法非常「本土化」，懷疑有本地團夥參與，「有的騙徒會扮成義工，謊稱下周有活動，要求網上買旗，或者利用同情心，籌集醫藥費等等。」

◆圖為市民在公共地方使用電話。香港文匯報記者曾興偉 攝

有騙徒則要求賬號主人的朋友幫忙購買蘋果或谷歌商店的禮物卡，這些禮物卡金額通常不大，僅數百元，有卡號即可上網轉賣，容易脫手，被騙親友一般也不以爲意。「不過騙徒就是這樣的，開頭是小銀碼，聊天聊多了，掌握更多資料後，就可能獅子大開口。」

留意登入者裝置 雙重認證減風險

由於騙徒在發送索財信息後可以將聊天紀錄隱藏，用户難以察覺，甚至可能長期與騙徒共用賬號。方保僑建議市民應經常留意WhatsApp內的「連結裝置」，如果發現有可疑裝置連接WhatsApp賬户，應立即刪除。

WhatsApp是在香港較普遍應用的通訊平台，他建議用户盡量開通雙重驗證（見圖解），可減少賬户被盜機會，「未開通雙重驗證的話，如洩露一次性密碼給騙徒，賬户就會被盜；開通後，需要一次性密碼和賬户密碼兩項資料，才能操作賬户。」

就近日有網民反映，有騙徒假冒「WhatsApp公司」官方賬號，向該用户發送信息，信息內附含連結，只要不慎點擊連結，就有可能「中招」導致賬號被盜。方保橋表示，WhatsApp官方賬號名稱旁邊有「綠色勾號」，並寫有「WhatsApp官方賬户」，點擊賬户名稱，會發現它沒有電話號碼，即代表確是官方賬號，可以信任，若無以上特徵，則恐爲騙徒的僞裝。

◆香港文匯報記者 唐文、蕭景源

防騙貼士

如使用WhatsApp 網頁版

- 不要盡信搜尋器置頂的搜查結果，尤其那些標示為「贊助」的搜查結果
- 把常用的連結放入瀏覽器的書籤(bookmark)
- 點擊任何連結前亦應留意網址是否有異樣，例如串錯WhatsApp、域名怪異
- 如收到突如其來的轉款、借錢或經濟援助要求，致電對方核實清楚

「官網客戶」的白撞訊息

- 切勿胡亂點擊任何連結，或接聽不明來歷的電話
- 若未經查證，不應該披露個人資料
- 舉報並封鎖所有可疑訊息及電話號碼

其他建議

- 啟用雙重認證功能
- 登出所有不明的已連結裝置
- 不向任何人透露任何密碼或代碼
- 加強賬戶私隱設定，例如將不明來電設為靜音，限制他人查閱資料權限(上線時間、在線狀態等)
- 不向任何人透露任何密碼或代碼

◆資料來源：CyberDefender守網者（警方轄下的網絡安全資訊平台）

◆整理：香港文匯報記者 唐文

WhatsApp 雙重認證步驟