

打擊濫用公屋應「加辣」

房委會本月起收緊公屋富戶政策，住戶須每兩年申報物業和居住狀況，並於周二（3日）起分批按要求填寫申報表，首批8.8萬名住戶須於11月底前交回，否則有機會被中止租約。當局終於正視公屋資源濫用情況，態度值得肯定。然而，全球多年前早已踏入大數據年代，房委會依然原地踏步，使用上世紀的原始落伍辦法進行審查，不但難以確保將稀缺的公屋資源公平地分配到真正有需要的市民手上，長遠更會削弱政府公信力。

本港公屋資源長期存在嚴重濫用

情況，已不是什麼秘密，內地網民對此亦知之甚詳。近日有自稱來自四川的女子，穿着時尚性感，拍片介紹其與丈夫及女兒居住約600呎公屋單位，無遮擋全海景，採光十足，更有工人房，豪言「香港隨便打份工都兩萬」，令大批網民羨慕，因一般三人家家庭只能獲配約300呎面積公屋。有網民更發現，她早於2018年曾於微博分享其於深圳買入的400萬元人民幣逾2,000呎單位。

此等情況其實早已司空見慣，甚至成為不少影視作品的諷刺和取笑素材。

多年來立法會議員不斷要求房委會正視，但一直沒有下文。即使是今次新收緊的公屋富戶政策，住戶依然不需要填報其他非物業資產及境外物業，資產審查這兩大主要漏洞仍然存在。而且對虛報和瞞報的處罰亦非常輕微，例如今年6月和7月均有瞞報擁有私人物業而被定罪的公屋申請者，僅判監禁14日、緩刑12個月及罰款數千元，不痛不癢，必須「加辣」。

其實，在大數據年代，當局倘真想進行物業和資產審查，早已不需再利用紙張表格郵寄和填報這種原始、低效、

高成本的落伍手段。本港發展智慧城市多年，其核心是城市的數碼基建，其中「智慧政府」，就是將多方數據進行匯集，利用大數據技術進行管理應用。因此，當有人要求以政府公帑資助其入住公屋，政府理應有權履行公共利益守護者的職責，持續對其日常消費、用電量、土地註冊處成交紀錄等數據進行採集，借助科技力量，短期內便能推算出其資產狀況，接着只需向相關機構進行核查便可。內地近年對房產證的數碼化管理日趨完善，只要有心，要堵塞公屋資產審查漏洞並不難。

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。私隱專員公署昨透露，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用戶亦向本報表示，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。（相關資訊刊P5）

私隱專員鍾麗玲接受電台訪問透露，在約900名受影響人士中，有個案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。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。

WhatsApp用戶阿Paul昨接受本報訪問表示，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一萬元，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並非其姓名，故引起其朋友懷疑，致電向他查詢，他才知賬戶被「騎

WhatsApp被騎劫 洩近900人資料

5社福機構學校中招 騙徒冒用戶向親友借錢



■現今生活中人人機不離手，其中WhatsApp更是主要通訊軟件。

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，「已經認住過數畀我，但打嚟問入落騙徒提供嘅戶口，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，但有警員表示由於無金錢損失，所以只為其備案。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。

Telegram疑有同類騙案

除WhatsApp賬戶，Telegram用戶「蝌蚪」亦向本報透露其賬戶遭入侵。前日（4日），有人冒充他在賬戶內聲稱應急，向朋友借3,800元過數，還稱晚上會在櫃員機入錢還給對方，但其朋友知他不合如此借錢，有懷疑故斷然拒絕。與WhatsApp不同，Telegram未有屏蔽行騙



■騙徒盜取賬號後，向原號碼主人的親友借錢。

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。



■在Google搜尋「WhatsApp網頁版」，前幾位均是假冒網站。

專家倡刪除可疑賬戶「連結裝置」

香港資訊科技商會榮譽會長方保僑向本報表示，騙徒主要透過偽造虛假網頁版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。市民搜尋網頁版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。

本報記者嘗試在Google搜尋「WhatsApp網頁版」，發現結果靠前的位置均是假冒網站。在點擊連結後，會進入與官方相似的假冒介面，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。

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。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，要求人網上買旗，或者利用人同情心，籌集醫藥費等等。」他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賬戶，應立即刪除。

就近日有網民反映，有騙徒假冒「WhatsApp公司」官方賬號，向該用戶發送訊息。方保僑表示，WhatsApp官方賬號名稱旁邊有「綠色勾號」，並寫有「WhatsApp官方帳戶」，點擊賬戶名稱，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，則恐是騙徒偽冒。