

智能手機細細粒轉手好賺 內地客成賊人眼中「肥羊」

五一遊港

慎防樂極失機

香港文匯報訊（記者 郭兆東）智能手機型號愈出愈新，因體積細小兼價錢昂貴，長期成為賊人偷機轉手牟利的首位，更因存有大量個人私隱如聯絡人資訊及電郵，失竊後隨時洩露私隱連累親朋好友，結果不但破財，更令親友平白患上被詐騙之險。據香港警方數字顯示，去年街頭搶劫案急速上升，當中更以搶智能手機為主，扒竊案亦主要發生在人多擠逼地方，鑑於「五一黃金周」將至，內地旅客訪港隨時成為賊人目標，旅客務必要提高警覺。



■梁兆昌表示，港人手機私隱意識薄弱，容易被不法分子有機可乘。梁祖彝攝

豈只破財 洩密牽連廣

智能手機發展日新月異，由於「Mon」大機快又方便，令智能手機迅速滲透港人每日生活，機不離手已成港人寫照。但因智能手機體積細小，二手賣出價卻出奇地高，尤以型號愈新賣價愈高，令手機成為被搶劫及偷竊的「新寵」。據警方數字顯示，去年共有逾3.3萬宗盜竊案，當中有5,659宗涉及手機被偷，佔整體逾16%，更按年增加逾20%；另外搶劫案亦有435宗，同樣主要涉及搶劫智能手機，情況令人憂慮。

失工作記錄 兼職薪酬難追

手機被偷不但破財兼影響日常生活，更因現時智能手機內多存有大量個人資料，失機不再局限於個人問題，隨時牽

連甚廣。事主小薇(化名)

雖只是一名大學生，但同時是一名散工中介人，除了身兼多份兼職外，更管有其手下7名工人的工作及支薪記錄。「上個月行經旺角時，被數名陌生人碰撞後，突然發現袋中的手機不翼而飛，當下雖已即時回頭尋找有關人士，但人海茫茫一無所獲。」

「雖然已報警立案，但自知尋回手機的機會微乎其微。」她稱，遺失手機後，多份兼職的工作記錄全失，當中包括多份補習、超市收銀及私人助理，由於欠缺工作證明，難以向僱主索取薪酬，連同遺失的手機價值，合共損失逾萬元。「加上另外需支付予7名工人的薪酬，我只能自掏荷包先行支薪予7人，稍後再嘗試向有關僱主追討。」

憂資料盜用 冒詐騙風險

正是禍不單行，小薇的失機內同時存有大量工作上的聯絡資料，包括多位兼職人士的中英文姓名、電話及住址，同

時亦有多間公司負責人的私人聯絡電話及電郵地址，「電郵中亦包含不少網上購物的賬戶資料、信用卡號碼及單據，現在非常憂慮有關資料會被他人亂用，令他們蒙上被詐騙之險，故已即時通知有關人士停用信用卡以策萬全。」

手機資料流失可大可小，一旦電郵及個人姓名被盜用，隨時令事主墮入詐騙陷阱。據警方數字顯示，去年詐騙案共有6,923宗，按年上升12.9%，升幅多見於電郵騙案及電話騙案，其中涉及個人層面的電郵騙案，按年增加140宗至376宗，受害人被騙金額由數百元至逾39萬元不等；至於網上商業騙案中則有823宗涉及網上拍賣及購物；另電話騙案則有2,314宗，手法仍以「虛構綁架」及「猜猜我是誰」為主。鑑於「五一黃金周」將至，將會有大量內地旅客訪港，隨時成為賊人目標，一旦遺失手機，隨時「樂極生悲」，旅客務必提高戒備。

手機資料防洩錦囊

日常防禦工作

- 避免記錄敏感資料如銀行賬戶號碼、登入名稱及密碼
- 即使必須記錄有關資料，亦要以「強密碼」加密資料
- 定期為手機資料進行備份，並存放在安全地方，切忌與手機同放

何謂「強密碼」？

- 不會是字典中能找得到的英文詞彙
- 密碼必須易記，例如將記憶深刻的事件或人物，以密碼形式呈現
- 要有一定長度，並包含英文及數字，字元數達8至10以上更理想

如何揀選手機保安軟件

- 必須可阻擋惡意軟件入侵
- 偵測手機內程式安全漏洞
- 能定時為掃毒程序記錄備份
- 檢查新安裝程式的私隱權，防止應用程式取得不必要私隱權限
- 防止資料外洩

資源來源：香港電腦保安事故協調中心

製表：香港文匯報記者 郭兆東

方便「套」料牟利

香港文匯報訊（記者 郭兆東）

港人智能手機雖機不離手，但個人私隱保安意識嚴重不足，不但存有過量不必要資料，更未有裝上防盜軟件，簡單如鎖機密碼亦同時欠奉，隨時被不法分子有機可乘。香港電腦保安事故協調中心高級顧問梁兆昌警告，除一般聯絡資料外，近年不少市民傾向將手機當作記事簿，記錄每日行程細節、網上交易記錄及賬戶號碼連密碼，令手機價值不再局限於其本身機價，賊人得手後會將機內資料轉售牟利，令遺失手機的風險倍增。

缺保安意識 私隱存太多

今時今日智能手機當道，港人幾乎每人至少擁有一部，在車廂及街上埋頭玩樂，不過當中有不少市民對手機的私隱保安意識嚴重不足，不但在機內儲存不必要的個人資料，亦未有為手機裝上防毒軟件，避免黑客入侵竊取機內資料，更同時貪方便未有設定鎖機密碼，一旦手機被取去，機內資料將可「一覽無遺」。

就港人手機私隱意識低下，梁兆昌警告，由於手機功能愈出愈多，不少市民傾向將手機當作記事簿，記錄每日行程細節、網上交易記錄及賬戶號碼連密碼，並利用手機登入社交程式賬戶，甚至進行網上理財，但此時卻已經將賬戶資料及登入密碼記錄下來，令任何人只能取得手機使用權，便可隨時假冒機主登入賬戶，令機主蒙受不必要的風險。

同時，他又稱，由於機內存有的個人資料有價有市，只要有齊姓名及聯絡電話，便可轉手牟利，甚至有不法分子利用有關電郵資料，傳送惡意或勒索軟件，其禍害將可無限放大。梁兆昌提醒，市民在提防手機失竊的同時，亦務必盡快為手機安裝有保證的保安程式，及為解鎖手機定下「強密碼」，以便即使遺失手機亦可避免機內資料被亂用。

■手機一旦被植入該軟體，對方可隨時監聽通話及監看簡訊內容。網上圖片



近年盜竊案數據

年份	2011年(全年)	2012年(全年)	2011年首兩個月	2012年首兩個月	2013年首兩個月
盜竊案總數	35,026宗	3,3664宗	5,0542宗	5,522宗	5,113宗
盜竊案(搶掠)	391宗	435宗	70宗	66宗	62宗
盜竊案(扒竊)	1,583宗	1,540宗	299宗	328宗	280宗
涉及手機搶劫舉報宗數	486宗	527宗	/	/	88宗
涉及手機偷竊舉報宗數	4,691宗	5,659宗	/	/	776宗

資料來源：香港警務處

製表：香港文匯報記者 郭兆東

遙控巨響嚇賊

「保安盾」更「穩陣」

香港文匯報訊（記者 郭兆東）

智能手機一旦失竊，導致個人資料外洩後果可大可小，有電訊商為保障客戶私隱，推出「手機保安盾」服務，令客戶失機後可透過以指定號碼向電訊商發出短訊，遙距操控失機資料，並發出巨響嚇阻歹徒，及以GPS追蹤失機位置。有手機保安專家向本報表示，有關服務安全可靠，同時遠較經互聯網遙距操控手機可取，因所有指令均由電訊商發出，可避免有不法之徒藉此刪除客戶手機資料，造成不必要的破壞。

手機保安程式限制多

近年，市面上的智能手機多配備全球衛星定位功能(GPS)，不少軟件開發商為盡用有關功能，紛紛推出手機保安應用程式(如 find my phone等)，聲稱一旦機主遺失手機，可從網上登入私人保安賬戶，遙距封鎖或刪除手機內的所有個人資料，甚至可透過GPS追蹤失機去向。

香港電腦保安事故協調中心高級顧問梁兆昌在接受香港文匯報訪問時指出，有關程式限制

多多，首先需要失機連接互聯網才能開始追蹤失機訊號，再嘗試以流動數據連接手機的操控系統，假若手機被關上甚至位處沒有訊號的地區，有關功能即時報廢。同時他稱，若有關保安賬戶的登入資料落入黑客或不法分子手中，有關人士可隨時上網刪除所有資料，令機主平白冒上手機被重置及資料外洩的風險，最終得不償失。

電訊商遙控鎖機尋機

不過，對有電訊商推出的「手機保安盾」服務，梁兆昌認為較安全可靠，因客戶一旦遺失已安裝保安盾程式的手機時，可利用另一個指定手機號碼，向電訊商發出短訊求助，屆時電訊商將即時自動啟動「遙控鎖」功能，保護機密資料以免外洩，同時遙控刪除儲存於手機內的所有資料，再即時令手機發出巨響以嚇阻歹徒，及透過GPS追蹤遺失手機的位置。

他認為，有關程序雖較費時，但可避免手機內資料被錯誤刪除，因所有指令均要由電訊商發出，在保障個人所在位置不會被他人隨意追蹤的同時，亦能在便利與保安需要間取得一定平衡。