個人資料保護小叮嚀

近日來個人資料遭盜用與個人隱私遭受侵害的事件不斷發生，因此，當我們在享受資訊科技帶來便利生活的同時，應建立起重視個人資料保護的觀念，以降低個人資料被盜用的機會。以下簡略說明我國電腦處理個人資料保護法之規範，以及自我保護個人資料的方法。電腦處理個人資料保護法簡介 「電腦處理個人資料保護法」於民國八十四年公佈，其個人資料指自然人之姓名、出生年月日、身份證統一編號、特徵、指紋、婚姻、家庭、教育、職業、健康、病歷、財務情況、社會活動、及其他足以識別該個人之資料，更對公務與非公務機關蒐集、處理、與利用個人資料的情形，加以明文規範，如果個人資料被再利用的方式與當初取得時不同，需要取得當事人的書面同意，而且不能以概括方式取得同意，必須另外取得單獨的書面同意，確保當事人權益，以避免人格權受侵害，並促進個人資料之合理利用。

何時洩露了個人資料？

- 向政府機關申辦所得稅、申辦行駕照等。
- 使用網路進行購物、旅遊訂房、處理銀行帳戶。
- 加入各種團體成為會員或參與公益團體。
- 參加產品抽獎活動或填寫問卷調查領取免費贈品。 握有大量個人資料的單位，無法保證資料不會外流。

保護個人資料小秘訣

- 不在電話裡透露個人資料。
- 非信任之網站，勿隨意留下個人資料。
- 以碎紙機銷毀家中之各式帳單、收據、信件、藥單等。
- 不點選不明人士傳送的網址。
- 提防偽裝之網站頁面、電子報與信件。
- 絕不委託他人代辦貸款及信用卡。
- 影印證件時註明特定用途之用，不適用於其他用途。

網路攝影不設防，直播主角換你當

「出門在外，想關心一下家中的長輩， 於是登入居家安全系統來查看家中的情況」;「炎炎夏日，在外勤奮地跑了一天 的業務，為了回家時能有一個舒服的環境， 於是遠端啟動家中的冷氣機」;「出門旅遊，看見難得的美景，為了讓親朋好友也 能立刻欣賞到相同的景色，所以拍照留念並立刻打卡上傳雲端」; 這些在現代看似理所當然的服務，皆拜現今網路發達及科技進步所賜，讓我們平淡無奇的生活處處充滿了便利，但是，在這便利科技的黑暗面中，隱藏了什麼樣的危機呢？ 許多人都知道，現在居家防護系統非常多樣化，除了租用保全公司所提供的服 務外，熟悉電腦及網路架構的用戶也可以 購買相關設備，自行架設一套自己的防護系統，但這些保護居家安全的雲端設備， 該由誰來保護它的安全？近年來，網路攝 影機遭駭事件層出不窮，國外號稱擁有最多線上攝影機的網站《Insecam》，光是監看臺灣的攝影機就有四百多部（其中二百多部是落於臺北市區），而這個網站甚至依據攝影機的廠牌、架設地區、城市，以 及時區等項目進行分類，讓有特殊興趣的人士可以隨時選擇他們想觀看的鏡頭。那麼，當我們使用這些設備時，為避免隱私外露，該採取哪些保護措施？建議各位最 基本一定要做到的，就是將登入系統的密 碼更換為高強度密碼，另外亦需不定時地更新系統軟體，以及檢查連線紀錄，以避 免遭人監看而不自知的情況發生。

其次聊聊雲端家電的便利與風險，可連接雲端的家電，除了最常見的冷氣之外， 現在亦有廠商開發電動門、智慧電表、空氣清淨機、電鍋等智慧型連網裝置。這類家電的確可以為我們的生活帶來相當程度 的便利，達到節電、省時並提供舒適的生 活環境，但若此類系統設計有缺陷，難保 駭客不會運用這些設備來進行惡意攻擊。例如，在寒冷的冬天啟動冷氣並將其溫度調降至 19 度，進行無意義的惡搞；或是 竊賊趁家中無人時透過遠端搖控開啟電動門，趁機入侵住宅搜括財物，相信無人願意上述情況發生。那麼，我們該如何善用這些設備，而又不用擔心它可能隱藏的危害呢？商品生產者當然需要背負最大的防護責任，定時檢測並更新相關系統軟

體，而使用者務必 保護控制裝置的安全。舉例來說，若透過 手機使用雲端 APP 來控制家中的冷氣，那麼，這部手機就不要安裝太多應用程式； 再者，家中的智慧型裝置若是透過 Wi-Fi 進行連線，則 Wi-Fi 密碼也不應該設定的太過 簡單，以上兩點防護作為無需高超的電腦 功力，一般人應該都可以做到。

至於即時分享旅遊美景這類的行為， 究竟隱藏了什麼樣的危機呢？首先我們該考慮到，有哪些人可以看到我們上傳的照片，如果隨意一個路人都可以存取我們的 照片，那我們就不該上傳較隱私或者是背 景為機敏地區的照片。此外，亦應留心提供服務的供應商背景，還有使用前應詳讀 使用合約，因為某些公司在合約條款中提到，客戶上傳照片後，版權就屬於該公司 所有，他們可以任意使用，這類型的合約非常不合理，但多數使用者均未查覺，致 損害了自身的權益。另外，若決定使用這 類型服務時，仍應注意登入服務的密碼設 定是否安全，照片中是否夾帶 GPS 資訊等等，才能達到較佳的保護效果。整體而言，智慧型裝置已為現代生活 帶來了相當程度的便利，只是身為使用者的我們，除了懂得如何「用」以外，更該瞭解安全防護做法；好好保護自身隱私， 就不會成為最佳男（女）主角而不自知！

離線卻傳不明連結當心遭劫

即時通使用普遍，向來是駭客鎖定對象，包含自建帳號或劫持使用者帳號，在離線狀態卻傳送不明連結進行攻擊，資安專家提醒，如果使用者帳號密 碼遭竊，被利用來發送不明連結，務必更新帳號密碼，同時更新防毒軟體， 然後展開系統掃描，擺脫威脅。明明沒有登入即時通，卻還是發送奇怪連結給親朋好友，遇到這種狀況得注意，使用者的即時通帳號密碼是否遭竊用！賽門鐵克資深技術顧問莊添發分析，這些連結多是釣魚網站的網誌，目的是要來蒐集他人的帳號密碼，另外也可能是含有惡意連結網站，如果使用者的電腦沒有進行安全修補， 惡意程式可能會趁虛而入，至於傳送者則可能是駭客本人或是無辜使用者的帳號密碼遭竊取。

「這些傳送使用者，有可能是犯罪集團駭客自建帳號，或者一般使用者事實上因為他原本早就被網路釣魚，所以帳號、密碼被蒐集走了，或者是說 他被植入惡意程式，惡意程式竊取他的帳號密碼。」若使用者的即時通遭劫，專家建議，首要務必更新帳號密碼，然後更新防 毒軟體，並進行全系統掃描，以擺脫資安威脅。專家呼籲，網友平時不要 輕易點選來路不明的郵件與連結，定期更新病毒定義檔，防毒軟體最好具 備綜合性功能，包含網站防護可攔截惡意攻擊，才能安心遨遊網路。