# 網路揭露宣導案例-網路轉PDF洩密

使用網路轉檔服務要提高警覺！根據流傳於網路上的一篇文章指出，只要在Google鍵入「求職者編號 sharepdf」，即可搜尋到許多包括學歷、薪資證明、甚至公司的考核等資料，履歷表、薪資單、通訊錄，甚至機密文件皆一覽無遺！

經過搜尋，發現Google搜尋出許多人力銀行的履歷表，令人質疑是否為該等公司公開洩漏個人資料或遭駭客入侵所致。惟該文章指出，這並非人力銀行出錯或者駭客攻擊，而是求職者自行將資料上傳網路，究竟是哪裡出問題呢？

該文章作者指出，這些履歷表並非人力銀行外洩，而是從一個線上PDF轉檔網站「PDF Online」流出；作者還說，若以Google指定網站搜尋的語法「site:」進行尋找，則任何資料皆能盡收眼底，網友們不得不防。

作者指出，許多資料之所以在線上流傳，主要是因為PDF Online這個轉檔服務，使用者只要登上網，就可以把各種文件轉換成PDF格式，但無形中也增加了資料外洩的機率。也就是說，這些文件被公開，其實是當事人「自己同意」被Google搜尋公開的！該如何防止資料外流？最重要的步驟是在輸出檔案前，PDF Online網站即註明了資料可能被搜尋引擎找到，但許多人都忽略此點，進而導致珍貴文件公開。作者提醒，只

要改選下面的「Do not make my document public」，就可以防止類似事件發生。建議同仁少用該等網路服務，避免公務資料外洩。

資料來源: 臺灣桃園地方檢察署

# 淺談雲端儲存安全問題

雲端運算（Cloud Computing）是目前相當熱門的資訊技術，現今我們的日常生活已幾乎離不開「雲端」二字，而其應用之一的雲端儲存（Cloud Storage），與我們的關係更是密切，只要能連上網，使用者可以隨時隨地存取網路上的檔案，省去攜帶隨身碟、筆電的困擾；也不像傳統硬碟，若是不小心毀損或遺失，所有資料將付之闕如。對企業來說，雲端儲存服務能讓公司不必在自己的資料中心或辦公室內安裝實體的儲存裝置，而日常的維護工作可交給服務供應商；對一般使用者來說，雲端儲存大幅減少了舟車勞頓及運輸的成本。

搭著這股熱潮，業者紛紛推出雲端儲存服務來搶雲端市場這塊大餅，包括 Dropbox、Google Drive、AppleiCloud、MEGA 以及國內的中華電信 Hami＋個人雲和 Asus WebStorage 等，這代表我們所能選擇的雲端儲存服務非常多樣化。惟一般人在選擇或使用雲端儲存服務時，優先考慮的往往是它的儲存空間有多大、使用介面是否便利，卻忽略了雲端儲存服務潛在的安全隱憂。使用者也許認為雲端技術相當成熟，所以放心地把一些重要或私密的檔案和資料放在雲端上，但這可能還是防不住有心入侵的駭客。舉例來說：2014 年 8 月 31 日晚間在美國的 Reddit、4 chan 網站流出大量好萊塢女星的私密照片，造成網路上一片恐慌，雲

端技術安全備受質疑；其實這些照片是駭客經由 Apple iCloud 的漏洞入侵所盜取，即便是運行多年的 Apple iCloud 服務也存在漏洞。根據趨勢科技的分析，上述事件的發生有以下幾種可能原因：

一、使用不安全、易遭駭客破解的密碼：使用與個人資訊高度相關的密碼，相當容易遭到破解，駭客只需找尋相關資訊即可盜取資訊。

二、受害者未啟用 iCloud 的雙向認證：當攻擊者知道受害者的 iCloud 電子郵件地址，攻擊者就可能透過「忘記密碼」功能進行密碼重置。因明星多數的個人資料可從網路上取得，包括寵物名稱等等，大幅提升帳號被入侵的可能性。

三、攻擊者侵入另一個安全性較弱的帳號，以接收 iCloud 的密碼重置郵件。

四、重複使用相同密碼：許多人常在多個服務使用相同的密碼，若其他網路服務的帳號已被入侵，則 iCloud 的帳號也可能遭受攻擊。

五、網路釣魚：攻擊者發送針對性的釣魚郵件給明星，引誘她們輸入自己的 iCloud 認證資訊到假的登入畫面，藉此蒐集帳號與密碼。

除此之外，當我們在選擇各種業者所提供的雲端服務時，

必須在使用前看清楚其服務條款，否則這些服務也很有可能造成隱私上的隱憂；例如：Google Drive在推出時，其中一項服務條款便惹來爭議，內容為「當你將資料上傳或用其他方式提交到Google Drive後，你就給予Google（以及我們的合作夥伴）全球授權，可以使用、代管、儲存、再製、修改、建立衍生內容、溝通、出版、公開呈現，和遞送這些內容。」雖然Google表示使用條款中已載明內容的所有權歸用戶所有，但是並沒有保證只有在「為維持服務運作相關」的情況下，才可以使用部分的資料，這表示Google有更大的權利來操控我們所上傳的資料，這些內容甚至可能淪為廣告用途，因此，平時我們便需要做好個人資料的保護。以下列出幾種保護方式提供參考：

一、請使用強度高的密碼：千萬不要圖方便記憶而設置過於簡單的密碼，好的密碼應至少使用八個字元以上、英文大小寫與數字混合使用、盡可能包含一些特殊字元等；即使設置強度高的密碼，也不應重複使用此密碼，應定期更新密碼。

二、重要資料加密備份：資料需多次備份並加密，除儲存於雲端之外，應再儲存於本機端或私人的硬碟和隨身碟中，重要資料切勿只存在雲端中。

三、避免使用公用電腦存取個人資訊：使用完公用電腦時，記得在關閉網頁前先登出並刪除瀏覽紀錄。

四、慎防網路釣魚：網路釣魚是一種誘騙電腦使用者透過手機、電子郵件、網站或通訊軟體，竊取個人資料或財務資訊的手段。所以在收到任何簡訊、電子郵件時，需再三確認其內容，切勿輕易回覆。

雲端儲存服務固然方便，但卻無法保證其安全性。個人私密或重要的資料應盡可能避免儲存在雲端上，若要儲存，也必須做好加密保護的動作。科技發展是一體兩面的，以雲端儲存服務而言，在運用其方便性之餘，我們也應正視它所帶來的安全議題，才能享用科技而不淪為駭客的目標。

資料來源: 臺灣桃園地方檢察署

## 離線卻傳不明連結 當心駭客或帳號遭劫

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，其後展開系統掃描，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帳號密碼是否遭竊用！賽門鐵克資深技術顧問分析，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，或者一般使用者早已被網路釣魚，所以帳號、密碼被蒐集走了，或是被植入惡意程式，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。

資料來源:臺灣桃園地方檢察署