網路轉 PDF 洩密案例

壹、網路轉 PDF 洩密

使用網路轉檔服務要提高警覺！流傳於網路上的一篇文章顯示，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！

經實際搜尋，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，啟人疑問者，究竟是哪裡出問題呢？

該文章指出，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，網友們不得不防患。

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。

貳、畢業校友的個人資料

周先生某日在網路搜尋「姓名&住宅地址」等關鍵字，竟然尋找到他 10 多年前於某大學環境工程所畢業校友的個人資料，此外還看到 1994 到 1998 年該校畢業校友的姓名、住宅地址、任職公司及住家、辦公室電話等資料，他覺得十分誇張了。覺得該校未做好資料保密工作，致洩漏其及其他校友的個人資料。

對此，負責網頁管理某大學環工所表示，該資料係 10 多年前的資料，當時校方無建置統一的網站，各系所自行在網路上找空間建立網頁，而資料都是由工讀生協助建立，後來由校方整併統一的網站，工讀生未將資料移交清楚才造成這個問題，已緊急將網路連結關閉。

依《個人資料保護法》規定，姓名、地址等屬於得以直

接或間接方式識別該個人之資料，建置資料的單位若有故意或過失，因而造成當事人個人資料外洩，可請求損害賠償，若無法證明實際損失，可請求 2 萬元以下的賠償。

參、機密文件勿亂丟

臺北市芋國中發生極機密的「高關懷學生名單」外洩事件，據聞係生教組長某日開完會後將學校中極機密的「高關懷學生名單」亂丟到回收箱，有老師不察拿來當廢紙使用，致學生看到這份高關懷名單，於是以智慧型手機拍下用社群軟體 Line 等四處流傳。而這份名單一共有十四名高關懷學生，有的學生被列為劣等學生，有的則是被列出有竊盜前科，有學生家長痛批，學校的疏忽讓學生的個人資料外洩，臺北市教育局要求某國中召開檢討會議懲處。

某國中主任說，對於學生看到這份高關懷名單，用智慧型手機拍下流傳，學校後續會加強學生的個人資料保護觀念。而學校也會加強機密文件的 SOP 處理，避免類似的個人資料外洩再度發生。學校對疏失的老師僅口頭告誡，臺北市教育局人員表示，這名老師並不是故意洩漏，學校的懲處是否過輕，會等報告送到教育局，再進一步檢討，而對於某國中發

生這樣的學生個人資料外洩，教育局也已經要求學校，針對這些個人資料遭外洩的學生輔導。

肆、安裝 P2P 軟體導致洩密

一、駐外人員公務家辦導致洩密

劉○○為中央某部會簡任主管，因職務關係經常接觸駐外館處重要機密業務，卻違反規定將公文電子檔以隨身碟複製後存放於住所個人電腦中；因該個人電腦有「FOXY」之 P2P（點對點）分享軟體，致該批重要資料（包括駐外管處上千件機敏公文，如「駐○○辦事處工作任務書」、「駐○○辦事處電報及公函」、總統出訪「○○專案」等核列為「機密」及「密」級公文）從網路洩漏，嚴重影響國家安全及利益。

二、公務家辦洩密戕害政府機關形象

某政府機關簡任主管○○○習慣將經手（包含屬下陳核及其他課室會辦）公文之電子檔拷貝留存備用，並經常以隨身碟再將其拷貝至家中電腦硬碟儲存運用。孰料，其家用電腦早遭駭客植入後門程式而不自知，以致長期大量經手之機密文書陸續外洩，直至我國情治單位查獲上情且依法偵辦時，其方

知事態嚴重卻為時已晚，事發後某民意代表召開記者會對其所屬機關嚴詞抨擊，經各媒體大幅報導，損害政府機關形象。

三、委辦業務管理不當資料洩密

某環保單位委外辦理之「柴油車排煙檢測站檢驗計畫」業務，係屬業務機密資料，惟承包該業務之公司員工劉○○，利用處理檢測站公務電腦安裝 FOXY P2P 軟體下載音樂，致電腦檔案中「全縣車齡 9 年以上車輛通知到檢名單及總清單」公務資料因自動分享而外洩，造成應保密之資料，仍在網際網路中流傳。案經本局透過網路搜尋軟體搜尋發掘，通報該環保單位政風室查辦，惟因對委辦公司並未訂定管理辦法及罰則，僅能要求委辦公司，將檢測站公務電腦中與檢測站業務無關之應用軟體刪除，並設定使用權限，以避免發生類似情事。

四、員警電腦公務資料洩密案

某警察局保防室發現該該分局偵查隊之重要資料（含「○○珠寶銀樓負責人陳○○遭強盜案偵查報告表」、「偵辦 1128 專案指示交辦案件管制表」外洩，而該等資料係由張○○、李○○等 2 員承辦，保防室高度懷疑該 2 人外洩。

案經該局資訊室人員於檢查偵查隊辦公室內所有電腦時，於

偵查佐張○○所使用之電腦中發現有網路卡 2 組執行程式，其中 1 組非公務電腦之網路卡程式（係自行外接網路）；另於其公務電腦 C 槽及 D 槽發現隱藏木馬程式、隨身碟、FOXY 等病毒及軟體，並發現該員公務電腦之檔案除未設密保護外，更任意開放網路分享權限，致承辦案件等機密文件外流，違反警察機關資料安全實施規定及個人資料保護法。

伍、機關網站洩密

一、詐騙集團利用網路洩漏之個人資料詐騙

本府所屬機關屢發生員工遭詐騙集團詐騙案，該等不肖份子以電話假冒本府某機關學校現職同仁或退休人員進行訛詐，以家人生病急需醫療費或為其預墊之保險費尚未返還為由騙得數十萬，後遭詐員工向現職同仁或退休人員本人聯繫始知受騙！經查察發現詐騙集團疑似由本府所屬機關網站或 Google 搜尋取得機關員工通訊錄，而該等機關網站管理者對於網際網路資訊揭露缺乏完整認識，致將含有姓名、電話、服務機關等未加密之個人資料放置於網路，而搜尋引擎(Search Engine)的網路搜尋及網路快取服務之資訊採集器(Robot/Spider/Crawler)、將其建立索引，然後把索引的內容

存放到資料庫，致使詐騙集團得以搜尋該等資料，進而進行電話詐欺。

二、網站留言板未適當遮掩個人資料

小李和鄰近住戶組成土地重劃自救會向某地政機關陳情，拒絕徵收所有土地進行其他開發，除於該機關網路信箱陳情外，一行人浩浩蕩蕩到該機關門前進行陳情請願，並遞交載有相關自救會成員身分資料之陳情書，經該機關派代表受理後離開，嗣後卻發現該自救會成員陳情書中的個人資料，竟成了該機關於重大重劃案件評估說明會之附錄資料，且該機關為求便利，又以網站留言板回覆陳情人，亦未適當遮掩相關個人資料，造成該自救會成員的身分證字號、電話、地址等個人資料全部公開在網站上可供人點閱、下載，該自救會立即電洽該機關抗議其作法失當，且違反相關規定，揚言告到底，並要求國賠。

陸、社群軟體 LINE、Facebook 詐騙案例

一、LINE 暗藏騙取臉書帳號、密碼的釣魚程式

邇來陸續有數百民眾，收到來自「新竹市政府官員、警員」的 LINE 訊息，內容是「我朋友在參加 YAHOO 攝影比賽」

後面還有人名與網址，收訊者誤以為參賽者就是發訊人的好友，點開網址，出現攝影作品，一旁還有「請使用 FB 登入投票」字樣。多人在未加思考下，幫對方投票按讚，登入臉書帳號與密碼後，還回訊給發訊人說：「我已經幫你朋友投票了喔！」,嗣後許多公務員與員警發現,自己明明沒發 LINE 給別人，竟收到一堆回訊，才發現事態嚴重，火速前往新竹市刑大科技犯罪偵查隊報案求助。經查此網頁是釣魚程式，歹徒藉由 LINE 帳戶夾藏訊息，任意發送出群組後，再騙收訊人進入假的臉書網頁，伺機獲取臉書帳號與密碼。這從被害人登入時，臉書跳出的字體竟是簡體字就可發現。

二、歹徒利用 LINE 進行小額詐騙

晚近許多民眾手機或 LINE 接獲「看著這些照片，好懷念以前的日子喔」、「朋友家狗狗參加人氣比拼，幫忙讚一下」，或者類似字樣並附上網路連結的簡訊時，一定要立刻刪除，若開啟簡訊中的網路連結，手機很可能已被植入木馬程式，遭到詐騙。

宜蘭縣縣議員接到陳姓女子陳情，指她 9 月 1 日收到「這是上次聚會的照片，你好好笑」簡訊，由於內有她的名字，不疑有他點下所附網址，打開後一片空白；10 月 15 日她又接

到「看著這些照片，好懷念以前的日子喔」簡訊，覺得有異，不敢再按連結，連忙向中華電信調帳單明細，發現被扣 1 千元行動電話費用。因是透過手機小額付款功能行騙，很多民眾不察，因此上當。

陳小姐曾向電信公司反映，卻僅回覆已轉請加值廠商處理，要不然可以去報警。議員建議電信公司應該主動處理，勿成為詐騙集團的幫凶。類似詐騙方式從 9 月起在宜蘭縣出現 24 件，詐騙總金額 6 萬 3800 元，受害者最多被騙走 7 千元，少則 1 千元。電信公司表示，近來確實發現小額付款金額暴增，用戶若有異常扣款情形，可持帳單洽各服務中心查詢，若確遭詐騙，將為民眾簽結取消；若已付款，會協助向加值廠商催討。

三、Facebook 購物社團詐騙

你知道嗎？社群網站 Facebook 有一項十分奇怪的設定：只要有人邀請你加入社團，無須你的同意，就會自動成為該社團成員。或許 Facebook 的本意是方便社團的推廣，然而許多「購物社團」反過來利用這項設定（或可說是漏洞），快速任意拉人進入社團，製造業績；而新的詐騙手法也應運而生。

首先，詐騙集團會利用「購物社團」的便宜貨品吸引你上門。由於購物時本來就要附上個人資料，包括住址、電話等，對方可能會以「任何理由」讓你上當，要你提供「簡訊認證碼」給他，聲稱這樣方便交易的進行。一旦你提供了，不但可能收到大量金額的帳單，詐騙集團也可能直接拿去當人頭戶利用，後患無窮。

事實上，不管對方是不是詐騙集團，網購都有一定的風險；由於台灣的網路交易環境不算健全，建議民眾購物時要找「超高評價」以及「有實體店面」的店家會比較保險，且貴重物品最好直接去店面購買，或找人陪同見面交易，當場檢查貨品，降低交易風險。尤其 Facebook 不可能擔保民眾購物的安全性，也不會介入，因此必須格外小心。