機密維護常識彙編（101 年 5 月份）

＊電子郵件停看聽

壹、電子郵件的黑暗面

電子郵件是 21 世紀現代社會重要的資訊傳送管道，現代人透過電子郵件進行資料傳輸、溝通訊息、處理公務、聯絡感情等，是便利且迅速的資訊交流方式。但是隨之而生的電子郵件安全性議題，從許多媒體及資安事件中，發現電子郵件已成為發生資訊安全事故的重要傳播載體。

社交工程(Social Engineering)是以影響力或說服力來欺騙他人以獲取有價值的資訊。駭客以電子郵件為載體結合社交工程的攻擊手法，近年來一直是造成企業或個人威脅和損失的主要原因。這種攻擊手法造成的威脅，在於有心人士不需具備頂尖的電腦專業技術，只要企業員工對於防範詐騙沒有足夠的認知，就可輕易地避過企業的軟硬體安全防護。這些有問題的電子郵件附件中常夾帶病毒、蠕蟲、木馬程式、傀儡程式等惡意程式，或是在信件本文中夾帶惡意連接、網路釣魚、偽裝成知名企業或機關單位寄發的電子郵件，通知收件人必須重新驗證密碼或登入某網址輸入個人資料等等手法，而取得各項帳號密碼、個人資料、財務資料或公司重要資料等資訊。

貳、不得不看的使用須知

維護電子郵件的安全不僅僅只針對您的帳號設定「安全」的密碼而已，以下幾項說明或可幫助您確保在使用電子郵件上的安全。

一、使用任何電子郵件軟體前，必須確認以下認知：

1. 避免在不安全的網路環境使用電子郵件：儘量避免使用公共場所的電腦收發電子郵件，很可能由於該設備被植入鍵盤側錄程式而造成帳號、密碼等資料外洩。有些瀏覽器被設定成自動留下 Cookie 紀錄，若使用公共場所的電腦完畢，必須記得清除自己的使用紀錄及敏感資料，以免有心人士竊取或登入冒用。不管在任何情況下，儘量不要在沒有經過加密的連線環境下讀取您的電子郵件；明文傳輸的網路環境，隨時都可能讓有心人士竊取您的電子郵件帳號及密碼。

2. 建立電子郵件驗證機制：市面上有許多商用軟體及免費數位簽章軟體可用，可在您所發送的電子郵件中加上數位簽章，機關(構)或公司也可依據需求自行建置 CA(Certification Authority，憑證授權)提供服務。如果您使用了 PGP(Pretty Good Policy)或 GnuPG(GNU Privacy Guard)之類的加密工具，將您的電子郵件加上數位簽章，那麼擁有您公開金鑰(Public Key)的收件者便可以確認這封信是由擁有私密金鑰(Private Key)的您所發送的，因此您必須妥善保管您的私密金鑰。在進行身分認證時請進行加密，理由很簡單，若您在未加密的情況下進行身分認證，可能會遭到駭客竊取您的帳號密碼，之後，駭客便可以使用您的帳號密碼收發電子郵件，或者將您的帳號密碼賣給垃圾郵件廠商或其他有心人士，用您的帳號發送郵件給其他人。
3. 以純文字模式開啟信件：不要讓電子郵件軟體使用 html 或 xhtml 網頁格式開啟信件，如果您的電子郵件軟體是使用 Microsoft Outlook、Outlook Express 或是 Mozilla Thunderbird 時，您應該設定電子郵件不以 html 格式打開，而以純文字的方式開啟。因為當您的電子郵件以 html 格式打開電子郵件的同時，可能會被駭客利用，甚至植入惡意程式。因此，筆者建議不管使用何種郵件軟體，請設定成以「純文字」的方式讀取電子郵件。可參考前圖 Microsoft Outlook 2003 的操作畫面。
4. 關閉「自動完成」的功能：許多電子郵件軟體都有提供「自動完成」的功能，我們也發現許多意外出現在選取收件者時發生。例如在 Microsoft Outlook 的收件者欄位中，我們常可看到 Outlook 會跳出下拉式選單讓我們選取收件者，不過有時候會選到排序上相鄰的聯絡人。如果今天這封電子郵件是要討論相當機密的事情時，發生選錯聯絡人的情況是相當嚴重的。

二、收發信件時必須注意：

1. 如果資料的私密性對您而言是相當重要的話，請使用信任的 POP3(Post Office Protocol 3，郵局協議版本 3)和 IMAP(Internet Message Access Protocol，交互郵件訪問協議)收發信件：如果電子郵件內所包含的資料對您而言是相當私密

的話,請避免使用 Web-Based 的電子郵件服務,像是 GMail、Hotmail 以及 Yahoo! Mail…等等。即便是該電子郵件服務廠商所制定的政策，對用戶隱私已有相當程度的保護宣告，但電子郵件服務商員工的行為不是我們所能控制的，網路上就曾出現員工將客戶的電子郵件帳號賣給發送垃圾郵件廠商的案例。

2. 發送給多人的郵件時，請將收件者以*密件副本*方式傳送：若是將朋友的電子郵件地址，在未經許可的情況下分享給他人是不禮貌的。如果您每次寄信給許多人時，都是將收件者放在「收件者」或者是「副本」欄位，如此一來所有的收件者都會看到其他人的電子郵件地址。若是將收件者放在「密件副本」的欄位，則每位收件者只會看到自己的電子郵件地址而看不到其他人的。
3. 請再三確認電子郵件中的收件者，尤其是使用 mailing list 群組時：有些人當收到 mailing list 裡面的電子郵件後，會按「回覆」以發表自己的意見，而這封電子郵件會直接回覆給 mailing list，讓 mailing list 中的其他人看到您所回覆的內容。倘若今天您加入某個 mailing list 中，而回覆這封 mailing listh 則有可能對上百人洩漏您的秘密。

三、平時注意事項

1. 請將電子郵件存放於安全的地方：當您收到加密過的重要私密郵件時，您會將這封郵件進行解密後以明文的方式儲存在您的機器中。記得將資料存放在安全的地方，若您的電子郵件服務商或您的機器所處的網路環境不夠安全的話，這些郵件的內容便有可能外洩。此外，定期備份郵件信箱的資料，刪除不重要及過時的郵件，以騰出較多的空間，才能維持個人電腦的運作效能。
2. 不要公開私人的電子郵件帳號：在這個世界上只要是分享他人使用的任何電子郵件，都有可能成為垃圾郵件廠商的目標，有可能將垃圾郵件寄送給您，或在寄件者欄位偽造成您的電子郵件位址發送郵件。若有越來越多的垃圾郵件廠商或釣魚網站偽造成您的電子郵件地址，導致您的電子郵件地址被 ISP(Internet Service Provider，網際網路服務提供者)阻擋，勢將造成您在使用電子郵件上的困擾。

參、最後的小小提醒

職場上對於電子郵件的安全管理，可於員工任用合約、規範、員工訓練、宣導…等多重管道中宣導，要求配合並落實安全使用電子郵件。實務上我們發現電子郵件的便利性也容易讓人公、私務混用，但電子郵件存在的威脅是不論公務或私務，正確使用電子郵件及相關操作，才能避免被駭客利用社交工程等手法入侵得逞。

近年來迅速走紅的網路即時通訊(如 MSN、Yahoo Messenger…)其便利性眾所周知，方便之餘相對也帶來潛在威脅，已逐漸成為電子郵件後的另一項入侵管道，諸如惡意網址連接、蠕蟲模式的攻擊等手法。唯有加強使用的安全性認知，不查閱、轉寄來路不明的郵件，更不任意點閱不明的連結或開啟附件檔案，再配合相關安全性的設定，才能有效減少受到惡意程式的入侵及攻擊。正確使用軟體才能享受網路帶來的便捷，避免自己成為被駭客入侵的下一個目標。

＊保護個資小撇步

壹、前言

高雄縣某治安機關一名組長私自將線民資料存到隨身碟後用私人電腦使用該檔案，卻因電腦裡有使用 FOXY，造成線民資料外洩；社交網站「臉書」也傳出受歡迎的應用程式可能會將用戶的資料分享出去，造成個人資料外洩；玉山銀行辦理網路銀行業務時，因未落實資安管理導致客戶資料外洩；臺灣銀行也傳出舊票據、存摺外洩，引發公司行號的恐慌，擔心印鑑可能會被盜刻。

媒體上不時播報著個人資料外洩的新聞，究竟什麼是個人資料呢？在現今資訊發達的社會，我們又該如何保護自己的個人資料不外洩呢？

貳、如何避免個資外洩

在探討如何避免個資外洩之前，我們應先了解什麼情況下會造成個資外洩。常見的類型諸如向政府機關或金融機構申辦各種業務、每個月收到的帳單明細、ATM 交易收據、各種網路行為、過於簡單的帳號密碼、送修電腦手機等含有儲存裝置的 3C 產品、向商店或俱樂部等申請加入會員、參加摸彩活動、路上隨機的問卷調查等等，都是造成資料外流的可能原因之一。

個人資料可能外洩的管道這麼多，我們該如何減低資料外洩的機會呢？

一、申辦政府機關、金融機構或其他機構之各種業務，需要提供個人資料以及身分證等證件，務必確認需在所繳交的證件影本上註明「僅供申辦○○業務使用」，以免不小心外流時被不肖分子移做他用，使自己成為人頭帳戶。

二、每個月的帳單明細、ATM 交易收據、申辦各項業務作廢的申請書或其他任何記有個人資料的便條紙，只要是記有個人資訊，即使只是隨手寫下的便條紙，都應小心處理。常見如使用碎紙機處理，若無碎紙機時，也應將重要資訊部分重複撕毀，切勿隨手丟棄。

三、隨著資訊的發展，透過網路行為所造成的資料外洩也有逐漸增加的趨勢。除了來路不明的網站別亂點擊，以免被植入惡意程式之外，所使用的瀏覽器也必須符合 SSL 或 SET 的安全標準，這樣才能確保在網路上進行交易時的資料是經過加密處理的；此外，P2P 等分享軟體所造成的「個人資料分享」也是時有耳聞，在使用上也必須特別小心。

四、勿用過於簡單的帳號密碼，無論是提款卡的密碼、網路上各項服務的帳號密碼，請勿用生日、電話、身分證字號等容易識別個人身分的字串，以免當卡片遺失或是帳號被盜取時，密碼被輕易地猜測出來。

五、近年來因送修含有儲存裝置的 3C 產品所造成的個人隱私外洩事件，教人不得不警惕。若因故障需送修時，應確保個人相關資料已妥善處理，亦或請維修商簽訂切結書切結不會盜用個人資料，以避免資料外洩。

六、申辦加入會員，在提供個人資訊前，應詳閱說明及相關保密政策，是否有選擇不將資料提供給其他廠商的欄位，以免個人資料不當流出。

七、參加摸彩活動、路上隨機的問卷調查，這些看似不經意的資料填寫，常常讓我們在不自覺中將個人資料流出，所以在填寫時應盡量避免填寫重要的個人資訊，留下的資料越少越好。

三、結語

個資外洩防不勝防，除了平時應養成良好的習慣外，切勿隨意提供個人資料並避免不當的網路行為，而在提供個人資料以申辦各項業務時亦須十分小心；當遇到疑似詐騙電話時，更應冷靜以對，小心求證，切勿驚慌，以免造成更大的損失

＊遊戲手機藏毒五步驟自保

趨勢科技指出，月初在大陸的Android第 3 方應用程式商店，發現藏於手機遊戲「Coin Pirate」中的惡意程式，一旦手機遭感染，簡訊中的個資會曝光，簡訊費用也可能暴增。

趨勢科技表示，偵測到的這隻木馬程式名為 ANDROIDOS_PIRATES.A，會隨著使用者下載「CoinPirate」這款遊戲程式感染使用者的智慧型手機；目前「Coin Pirate」已下架，但網路世界無遠弗屆，仍要提醒不小心下載的使用者注意。

過往類似的惡意程式會使用原始碼過濾受害者手機接收的簡訊，而這次的惡意程式則透過監測簡訊中特定關鍵字，像是 cash、money 等，來收集個資，將特定簡訊、國際行動設備識別碼（IMEI）與國際行動用戶辨識碼(IMSI)，相較於以往的惡意程式更具有針對性；還會利用受害者手機轉發簡訊，使受害者付出大筆的簡訊費用。除此之外，這隻木馬程式會將特定網站，以書籤的方式標註於受害者的手機網頁瀏覽器上；這些特定網站不排除藏有其他惡意程式，恐增加受害者瀏覽後中毒的機率。

趨勢科技建議，使用者在安裝任何應用程式時都應謹慎小心，請仔細閱讀程式說明，確定此程式要求使用者授與的權限是否合理。

使用者可以透過下列步驟，檢查自己的手機是否已經遭到這個惡意程式的感染：點選智慧型手機的「設定」，選取「應用程式」中的「正在運作的服務」，若發現有名為「MonitorService」檔案的存在，則手機已經遭受感染。使用者可以手動刪除此一惡意程式：選取「設定」→「應用程式」→「管理應用程式」，然後刪除此程式。

Android 平台的智慧型手機快速普及，而針對性的惡意程式也更多，Android 智慧型手機用戶可用 5 個簡單步驟自保：

1、確實使用 Android 平台提供的基本手機防護：設定 pin 碼或是開機密碼等，可以讓手機與資料受到基本保護。

2、盡量避免使用 Wi-Fi 自動連線功能：連上開放性的網路服務，如 Wi-Fi，看似相當便利，但此類網路的開放特質如同雙面刃，會讓使用者手機中的資料暴露在輕易被有心人士竊取的風險中。

3、在下載來自第 3 方應用程式商店的應用程式(App)前，請審慎考慮。

4、當有程式或網頁請求授權時，請詳細閱讀其請求授權的內容。

5、安裝具有信譽且有效的智慧型手機防毒軟體，以保護 Android 裝置免受惡意程式威脅。

＊警官勾結徵信社洩漏秘密資料案例

警政署刑事警察局預防科警官馮○○涉嫌多次利用職務機會，進入警政署電腦系統，查詢與其業務無關的多筆民眾刑案、車籍、入出境等資料，並洩漏給友人知悉，事後遭刑事局查獲移送偵辦。台北地檢署偵結後，依妨害秘密罪嫌起訴馮○○。檢方並以馮員係連續犯，向法院請求加重其刑。

據了解，刑事局督察室日前接獲檢舉，指稱馮○○疑涉勾結徵信業者、律師，利用職務機會，擅自進入刑事局電腦系統，查詢民眾刑案及入出境資料，並洩漏與徵信社及律師。

經督察室全面調閱馮○○自 86 年至 89 年間在警政署終端工作站使用紀錄表、刑事局電腦資料查詢紀錄簿及電腦檔案後發現，馮員確實調閱大批與其業務無關的秘密資料，並有外洩情事。

督察人員遂約談馮員進行調查，馮員坦承有將秘密資料洩漏給友人，於是依妨害秘密罪嫌將馮員函送台北地檢署調查。但檢方調查時，馮員卻否認有洩漏機密資料情事。馮員辯稱，89 年 3 月間開始「春安工作」期間，有林姓、吳姓警界同仁希望他提供一些失竊機車等資料，他並無將秘密資料外洩與友人。不過檢方依據刑事局督察室的調查筆錄、資料，認定馮員確有洩密情形。（以上資料轉載於臺中高等行政法院）