機密維護常識彙編（101 年 11 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的。

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，郵局通訊協定 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。

＊臉書詐騙多別再用傻瓜密碼

「我的臉書帳號被盜用了，請朋友們不要被騙」，許多人最近上臉書都發現此警訊，台中警方也受理多件臉書詐騙案，警方和臉書業者都提醒使用者，儘快更改密碼，不要再用自己生日等簡單的「傻瓜密碼」，以免帳號被盜用。

台中市警局刑警大隊科技犯罪偵查組長張承瑞表示，台中警方已受理多件臉書詐騙案，許多臉書使用者不知朋友帳號被盜用，誤以為對方是自己臉書的朋友，對方謊稱家中發生急難，需現金急用，匯款後沒有下文才知被騙。

警方另受理臉書詐騙案，歹徒同樣盜用別人臉書帳號後，從被害人臉書朋友群中找下手對象，先和被害人打招呼，再謊稱自己目前不方便使用手機，要求被害人手機接收簡訊再告知即可，被害人認為只是舉手之勞，卻因此被騙。

前台中縣副縣長張壯熙，臉書收到一名記者要求幫忙手機收簡訊，張壯熙敷衍對方後，歹徒氣得飆「髒話」，張壯熙還平靜的回覆：「我認識的這名記者不會罵髒話哦！」

張承瑞說，歹徒要求被害人手機接收簡訊時，可能正在做線上付費、購物，歹徒問出被害人電話號碼，輸入後，小額付費的網頁會傳一封認證碼到被害人手機，等被害人告知歹徒此碼，歹徒即可「免費」購物，最後由被害人付費。

警方說，有歹徒專找臉書密碼簡單者下手，先進入被害人臉書個人資料欄，以生日等數字或英文字母嘗試輸入密碼，若輸入正確，就可盜用對方臉書帳號行騙，歹徒稱這種簡單密碼為「傻瓜密碼」。

張承瑞表示，臉書可透露太多個人訊息，例如職業、住址、生活背景，台中警方就曾偵破一件擄人勒索案，被害的大學生在臉書上無意中說出自己家境富裕，歹徒透過他的臉書親友資料找到大學生住址並押走。（聯合報／記者游振昇／台中報導）

＊機關員工不慎洩漏民眾個資案例

案例 1：某機關員工張○於本(99)年 8 月某日近中午時分，接獲一名自稱該機關前首長的電話，要求查詢被開立無照駕駛罰單之○○○等人（均僅知身分證字號）之駕照是否遭吊銷？張員表示待查證後再回覆，惟對方一再催促致一時失察，遂

委請不知情之同事以其帳號密碼進入電腦主機資料庫查詢，並由張○電述提供有關○○○等人之姓名及價籍地址。嗣張○察覺有異，主動向直屬長官報告並經向前所長查證表示未曾電詢，始知受騙。

案例 2：○○分局○○派出所警員李○於 99 年 8 月某日晚間 7 時至 9 時，擔服值班勤務，接獲警用分機來電，對方自稱係偵查隊學長○○○，並稱因電腦無法連線登入警政署警政知識聯網 E 化報案系統，請渠代為協助查詢失竊車輛車籍資料共 7 筆，並向李員表示，如工作忙碌將改向勤務中心集中查詢所需資料，李員認該員熟稔警察機關內部用語，而誤認該員亦係警職人員，即將所交查之車主相關資料回報該假冒學長者，事後察覺有異，致電該分局偵查隊查證並無其人，李員自覺恐已不慎洩漏民眾個人資料，即主動將上情陳報所長，嗣由該分局調查後函送偵辦。

＊善用科技發明、做好安全防護

現代的科技技術，無論是日用品或資訊產品，相互結合，可以產生更大的效用，在我們的傳統印象裡，要做好環境安全防護，無非是買個鎖將大門鎖起來，窗戶要關好，但是這種防護措施容易被破壞，而且不留痕跡，想事後追查破壞入侵者都很難。假如我們能善用現代科技發明的產品，尤其是電子化、資訊化的產品來做為安全防護的設施，可以大大的提高安全防護的能力，以有利於事後的追跡。

本府的安全防護，雖有相當的人力與科技設施防護，但由於本府是一個開放性的為民服務機關，當民眾進入本府後，現有的安全防護措施就有賴各單位的安全防護措施來輔助，以形成嚴密的安全防護網。本府各單位的安全防護措施普通不受重視，少有單位能注意並實施自己單位的安全防護。事實上，只要我們能善用現代科技發明的防護產品，除了能有效的維護安全外，對各對位的日常作息也不會產生不便，是值得我們去推廣的。

一般來說，可利用電子科技設備來維護辦公室安全項目，包括門禁管制、防盜監視、錄影監視、緊急求援、消防安全等。

門禁管制：無論是使用門禁管制卡或指紋或瞳孔辨識器，管制系統將會偵測任何非法入侵者，並同時觸動警報系統或透過電話撥叫有關人員做出緊急應變。

防盜監視：對於環境週邊，如窗戶、通風口、頂樓、後門、側門、逃生門等的防護需求，可以設置防盜監視器，啟動偵測系統，除了可以監看四週環境外，也可以留下記錄，有任何的異常亦能啟動報警系統。

錄影監視：錄影監視除了可結合前述防盜監視，錄影存証案發當時的現場情境外，可在不同的角度即時察覺異狀，且可因環境的不同，禁設不同的攝影機，消滅監視死角。

緊急求援：在需要的地方，可以裝設求救按鈕，除了可以在現場發出警報信號以產生震懾作用外，也可以連線到自動報警系統，於緊急時向外求援。

消防安全：室內可以安裝煙霧偵測、瓦斯偵測等系統，於發現有異狀除自動滅火功能外，另可即時發出警報，以便及時防範火警發生。

電子化的防護設備，可以減輕人力負擔又可發揮比人力監護更強大的功能，為維護辦公環境之安全，可以考量逐漸的裝設，多一份準備少一份災害，我們期待全體同仁共同為本府安全防護提供建言，更希望大家攜手共同維護。