有關網路、資訊、個資之「你問我答」

一、問：為何從某些電腦瀏覽機關網頁時，畫面一片空白，但有些電腦又可以？

答：可能原因為所使用的電腦中未安裝 Flash Player 所致，請至以下網址下載安裝即可解決：　http://www.adobe.com/tw/products/flashplayer/

二、問：如何正確顯示電子公佈欄各項訊息內的附加檔案？

答：本所網頁電子公佈欄中所附加的文件，如您無法正確閱讀文件內容，請至以下網址下載安裝即可解決：

PDF 檔案：Acrobat Reader http://www.adobe.com/tw/products/reader/

三、問：我的個人資料遭非法蒐集或利用，該如何處理以維護自己之權利？

答：按個人資料保護法（以下簡稱本法）第三條第七款規定：「非公務機關：指前款以外之左列事業、團體或個人。

(一)徵信業及以蒐集或電腦處理個人資料為主要業務之團體或個人。

(二)醫院、學校、電信業 、金融業、證券業、保險業及大眾傳播業。

(三)其他經法務部會同中央目的事業主管機關指定之事業、團體或個人（目前經指定者計有：期貨業、中華民國產業保險同業公會、人壽保險同業公會與台灣更生保護會）。」準此，非屬上開規定之民間行業、團體或個人，尚無本法之適用，合先敘明。

次按，本法第七條及第十八條分別明定公務機關及非公務機關須符合特定要件，始得蒐集或電腦處理個人資料，至於利用所蒐集之個人資料亦需依同法第八條及第二十三條規定辦理。不論公務機關或非公務機關，如有違法蒐集或利用個人資料情事者，依本法第二十七條至第三十條規定，得請求民事上之損害賠償；亦得依同法第三十三條至第三十五條規定，訴追行為人刑事責任。如違法主體係首揭之非公務機關，依本法第三十八條至第四十條規定，目的事業主管機關得處罰負責人罰鍰，其情節重大者，並得撤銷依本法所為之許可或登記。

四、問：我在貴所網站上申請預約接見需填入申請人身分證等資料，我的身分資料會不會在網路上被盜用？

答：預約接見須先檢核申請人之身分，因而網路要求輸入個人基本資料，而法務為了保護您個人資料之安全，在網路傳遞皆經過傳輸加密機制，以確保資料在傳輸過程中不被第三者非法擷取。

五、問：我想要在網路上查詢政府機關的法令及解釋是否可提供網址？

答：網際網路上法務部提供民眾查詢相關法令解釋之法規資料庫包括：全國法規

資料庫（http://law.moj.gov.tw/）及法務部主管法規資料庫 http://mojlaw.moj.gov.tw/），亦可經由本所提供之網頁連結快速進入相關網站，有關法令解釋收錄之範圍部分，說明如下：

（一）全國法規資料庫係由全國各機關將各主管業務對於各機關一體適用之行政函釋通報公布於全國法規資料庫入口網站之行政規則最新訊息區。

（二）法務部主管法規資料庫則收集了法務部主管業務及部分相關業務機關之行政函釋。

以上所提供查詢行政函釋之管道，歡迎您多加利用。

六、問：什麼是垃圾郵件？有何害處？

答：

（一）所謂垃圾郵件（SPAM）意指：

1.垃圾郵件，顧名思義就是不請自來、有商業企圖的 E-mail。

2.垃圾郵件，是某些想利用 Internet 致富的人，藉以散播廣告或色情的媒介。

3.垃圾郵件，是一份內容相同的郵件，未經收件者同意，即大量散發的郵件，信件內容多半以促銷商品為意圖。

4.嚴格說起來，垃圾郵件，是一種剽竊行為。傳送 Mail 者只需花極少的金錢，即可造成收件者龐大的損失。

（二）垃圾郵件的害處如下：

1.垃圾郵件除了將使網路陷入動彈不得的境地外，更令人憂心的是其附件檔案可能夾帶的病毒，將同時大量危害企業網路。

2.其附件可能附贈 Java or Activex 等惡性程式，許多特落依木馬病毒（Trojan Horses）就是藉此大量擴散。您可以想像如果讓這些未經許可的垃圾郵件繼續為所欲為，將造成企業多大的損失。

七、問：如何判斷所收到的是垃圾郵件？

答：有以下數端可加以判斷：

（一）「天下沒有白吃的午餐」，當你收到各項難以置信的中獎通知、特價優惠…等好消息時，得提高警覺。通常這些發信者本身的 Mail address 也是造假的，也就是說當憤怒的收件者回信加以指責時，他們卻可充耳不聞。

（二）信件內容的文法或錯字百出。

（三）他們會要求收件者來電提出停止寄件通知。但這是另一個陰謀，當你撥出電話時，你會發現對方轉換另一個方式對你實行更強力的電話行銷，更糟的是，這會是個高計費的電話。

（四）大部分的內容為廣告及電話服務。

（五）他們會要求你若不想再看到此廣告請回覆。

八、問：什麼是網路詐騙郵件？如何辨識？

答：

（一）所謂網路詐騙郵件，係指冒用銀行名義所發出的電子郵件，讓使用者難辨真偽。提醒您千萬不要回應，並立刻刪除。

（二）辨識詐騙郵件之方法如下：

1.登入某冒用偽造的網路銀行時，除 ATM 卡號及密碼外，還要求您輸入其他機密資料。

2.寄發緊急、有時間限制或是要求您提供、更新或確認機密資料電子郵件，或要求您在 e-mail 的空格內，填入機密的個人或帳戶資料。

（三）更要注意的是，決不點選可疑電子郵件的連結網址。

九、問：什麼是網路釣魚?

答：網路釣魚是一種網路詐騙手法，多是利用偽造電子郵件與偽裝網站作為「誘餌」，讓使用者不自覺洩漏個人資料，成為垃圾郵件業者的名單；電腦也可能會被植入木馬程式，破壞系統或讓重要資訊遭竊。而最危險的情況是：誘騙使用者的銀行帳號密碼、信用卡號與身分證字號等機密資料，釣魚者再伺機偷竊金錢或有價資訊。網路釣魚所用的誘餌千奇百怪，包括偽裝成知名銀行或線上服務業者通知使用者資料過期、無效需要更新，或者是基於安全理由進行身分驗證，要求使用者重新確認銀行帳號密碼或信用卡號。只要使用者一時不察經由電子郵件指引的網址，就會成為受害者。

為了避免您受到網路釣魚的危害，請遵循下列基本指導方針：

（一）留意詢問機密資訊的電子郵件：其是與財務相關的資訊，金融機構及其他負責任的公司不會透過電子郵件要求機密資訊。

（二）請勿提供機密資訊：網路釣魚作者喜歡使用恐嚇的手法，他們會使出各種威脅說法，直到您更新特定資訊為止，應直接連絡商家，以確認要求的真實性。

（三）絕對不要透過電子郵件訊息內嵌的表單傳送機密資訊。

（四）如果您需要在網路上提交公司信用卡號碼或其他機密資訊，請確認該網站是安全的。請檢查網址，開頭應該是 "https://" 而不是 "http://"。

十、問：使用網路帳務服務時，如何自我保護？

答：

（一）設定網路銀行密碼時提高警覺：

1.避免選用容易被猜中的號碼或字母組合，例如出生年月日、電話號碼等。

2.切勿使用您在其他網路服務的帳戶名稱及密碼，例如電子郵件或網路簡訊，以免被有心人猜中。

（二）切勿向任何人透漏或寫下您的網路銀行理財密碼。

（三）養成定期更改網路銀行理財密碼的習慣。

（四）保護您的電腦。

（五）避免提供個人資料及金融資料。

（六）避免在公共電腦及網咖上進行任何網路銀行交易。

（七）確實核對網址【（https：//）受到網路安全機制的保護】

（八）妥善保管交易明細表。

（九）遠離來源不明的電子郵件，以免下載病毒程式或木馬程式。

（十）避免安裝來路不明的軟體。

（十一）安裝個人防火牆軟體，防止駭客入侵您的電腦。

（十二）安裝病毒檢測軟體，防止新型病毒入侵。

十一、問：使用網路時，有哪些安全訣竅？

答：使用網路時，有以下幾個安全訣竅：

（一）安裝個人防火牆與防毒軟體，並定期更新病毒碼，可防止駭客入侵您的電腦。

（二）詐騙郵件通常都是寄發緊急或是有時間限制，要求您提供更新或確認機密資料，因此切勿閱讀與開啟不明電子郵件，而應立即刪除此郵件。

（三）假網站就是仿造一般公司網站欄誘騙您洩漏機密資料的網站，為確保您連結至正確的網站，請直接鍵入正確網址或至搜尋網站直接鍵入公司行號全銜。