政府資通安全防護巡迴研討會

資安管理、法規及防護之經驗分享

有四個議程：

一、 政府單位推動 ISMS 經驗分享——檔案管理局

二、 電子化政府網路文官學院推廣說明會

三、 電子郵件之數位簽章辨識及社交工程演練結果－國家資通安全會報技術服務中心

四、 政府資訊公開法制對資安工作之影響－資策會科技法律中心

1. 第一個議程是有關 ISMS 的推動，ISMS 之前他們有開過課，我沒有去上過，所以對這個名稱有點陌生，後來才知道原來它是一種制度的制訂：

如何導入 ISMS 機制：

（1）步驟一：制訂政策

（2）步驟二：定義 ISMS 範圍

（3）步驟三：進行風險評鑑

（4）步驟四：進行風險管理

參考相關法規及規範 https://www.ncert.nat.gov.tw

2. 第二個議程是介紹電子化政府網路文官學院：

（1）提升公務人員資訊應用能力以及推廣電子化政府相關資訊

（2）負責電子化政府教育訓練及數位學習推廣

（3）政府機關數位學習之共用平台

（4）電子公文、office 系列、電子化政府、資訊安全、…等課程

（5）免費申請加入學習

Http://elearning.nat.gov.tw/

3. 第 3 個議程是有關電子郵件之數位簽章辨識：

（1）電子郵件之威脅

（2）社交工程演練結果

（3）判別郵件數位簽章有效性：

a. 可至hitrust(http://www.hitrust.com.tw)公司進行查詢—個人

數位憑證搜尋，輸入這封信的E-mail帳號，即會顯示憑證有效性

b. Outlook Express 對於含有數位簽章之郵件，會自動檢查錯誤。

c. 在 outlook 收信軟體中，請開啟一封含有數位簽章之郵件，並勾選「開啟郵件之前，警告我關於數位簽章電子郵件的錯誤」功能。

d. 當完成勾選後，若收到含有無效數位簽章之電子郵件時，在開啟或是回覆、轉寄此封郵件前，皆會自動會彈出警告視窗。

辨識郵件數位簽章之方式：

a. 先查看是否有數位簽章標記：信封上有徽章的標記

b. 確認寄件者是否為可信任的寄件人郵件位址。

c. 查看簽名者的 mail address 是否與寄件者相同。

d. 滑鼠移到右方數位簽章圖示上查看簽章是否有效。

e. 用滑鼠點擊數位簽章圖示，查看數位簽章是否顯示有效且受信任的。

f. 確認數位簽章資料之寄件者資訊和郵件主旨。

（4）無效及有效數位簽章區別：

a. 無效簽章會顯示錯誤；有效簽章會顯示確定已簽名郵件

b. 無效簽章會顯示錯誤資訊、憑證狀態顯示錯誤 X

（5）案例說明

如果平常有收到政治與情色郵件，最好請立即刪除，因為那些都是郵件的威脅，有夾帶病毒攻擊。

（6）結論：

a. 技術服務中心對外寄送之電子郵件均包含數位簽章

b. 不開啟寄件人之郵件地址不明或是未被信任之郵件

c. 不開啟收件人地址非本人之電子郵件

d. 不任意開啟未受信任之郵件檔案

e. 善用垃圾郵件信箱或是垃圾郵件判斷功能

f. 寄送不同收件人時採用密件副本的方式

4. 第 4 個議程是政府資訊公開法制對資安工作之影響

（1）於 94 年 12 月 28 日由總統公布實施「政府資訊公開法」

（2）政府資訊公開法之衝擊：

.政府資訊公開法明確賦予民眾資訊公開請求權

.行政機關之資訊必須要符合免除公開之事由，始得不公開

.人民若不服決定，得依法提起行政救濟

（3）資訊不當被 Google 公開時的處理：

.援用告知即取下之原則

.根據 Goolge 公布給網管人員的資訊，網管人員若不想讓自己的網站或部份網頁加入 Goolge 搜尋中，可在伺服器根目錄下放置一個 robots.txt 的標準文件，告知爬蟲不要下載內容

.Goolge 在其網頁上有提供避免資料遭爬蟲搜尋之結果

Http://www.google.com/support/