資安事件案例宣導簡報

電子計算機中心

96年9月7日

大綱

一、網站涉洩露師生個人資料
二、電腦失竊資料遺失
三、學生駭客竊取帳號修改網站
四、電子郵件帳號遭駭客竊取
五、公事家辦洩密(轉載自法務部)
六、8警所私灌FOXY偵查筆錄外洩(轉載自法務部)
七、全台近千網站被植入惡意程式
八、網路銀行資料遭竊取(轉載自刑事局)
九、涉國家安全研究領域教授之E-mail帳號遭盜用

一、網站涉洩露學師生個人資料(一)

案由：

中部某所知名大學網站因控管不當，透過Yahoo、Google等搜尋引擎，便可直接取得該校就學貸款學生名冊，名冊內含學生身份證字號、貸款金額等個人資料，讓學生資料暴露於危險之中。

一、網站涉洩露學師生個人資料(二)

預防方式：

(一)網站應指派專人管理審核內容，以避免洩漏學生、教師個人資料。

(二)不適合公開的檔案不可存放在公開之網站上。

(三)網站上過期的資料應進行檔案刪除、不可只移除超連結，以免被搜尋引擎取得而被讀取。

二、電腦失竊造成資料遺失(一)

案由：

南部某國小電腦遭竊，人事教職員資料因存放於電腦中而一併外洩、會計預算電子檔案亦於電腦中一同遺失。

二、電腦失竊造成資料遺失(二)

預防方式：

(一)行政業務資料應養成備份習慣，避免造成資料永久遺失。

(二)筆記型電腦、行動碟等儲存設備因攜帶方便、容易遺失，應設定密碼保護或資料加密，並儘可能避免存放機密公務資料，並妥善保管。

(三)辦公處所應加強門禁管制，設備遭竊應立即向所轄派出所報案。

三、學生駭客竊取帳號修改網站(一)

案由：

北區某知名高中之學生於駭客教學網站習得駭客入侵技巧，練習入侵多所學校網站，並於某小學網站發布『學校寒假延長訊息』假消息，另刪除多所學校網站重要資料。

三、學生駭客竊取帳號修改網站(二)

預防方式：

(一)校園應加強宣導駭客行為必須擔負法律責任。

(二)建置網站開發程式應加強系統安全(如輸入欄位必須進行字元檢查)，避免產生程式漏洞，遭駭客入侵。

(三)網站作業系統、資料庫、服務軟體(如 web Server)應定期更新軟體，避免系統漏洞產生。

四、電子郵件帳號遭駭客竊取(一)

案由：

國內4所大學之郵件伺服器與駭客中繼站建立連線，且特定電子郵件帳號遭登入下載郵件查看，疑似洩漏重要資訊內容。

四、電子郵件帳號遭駭客竊取(二)

預防方式：

(一)應注意電子郵件使用安全，勿開啟來路不明之信件，以免被植入後門程式竊取資料。

(二)郵件帳號及瀏覽器應取消記憶密碼功能，以避免帳號密碼記錄被駭客利用木馬程式竊取。

(三)個人電腦應安裝防毒軟體，且作業系統及防毒軟體應隨時更新，以避免漏洞產生。

(四)電子郵件及相關系統登入之密碼應定期更換。

五、公事家辦洩密（一）

案由：（轉載自法務部 ）

某中央政府機關內人員習慣將公文之電子檔案，以隨身碟拷貝至家中電腦辦公並儲存。因家中電腦已遭駭客植入後門程式，以致長期大量經手之機密文書外洩，又經各媒體大幅報導，損害政府機關形象。

五、公事家辦洩密（二）

預防方式：

(一)公務機密資料攜出應依程序辦理。

(依國家機密保護法規定：公務機密資料攜出辦公處所，應經機關首長核准)。

(二)家中電腦之使用較缺乏定期更新軟體與防毒程式之習慣，應妥善設定自動更新機制，以防範病毒入侵。

(三)家中電腦連線上網時通常沒有防火牆保護，應加裝個人電腦防火牆，以降低遭入侵之機率。

六、8警所私灌FOXY偵查筆錄外洩(一)

案由：（轉載自法務部 ）

據電腦犯罪防制中心指出：8所警察機關之警員擅自安裝FOXY(檔案下載軟體)於警所電腦中，且不熟悉FOXY之設定方式，誤將電腦中所有資料開放予所有人下載，造成警所電腦筆錄資料外洩，警政署怒追究相關人員的疏失責任。

六、8警所私灌FOXY偵查筆錄外洩(二)

預防方式：

點對點(P2P)檔案下載軟體因版本與種類繁多，軟體容易被改寫加入木馬或後門程式，故不要安裝P2P軟體，如Bittorrent(BT)、eMule、FOXY等，以免造成機密資料外洩；另P2P下載之檔案也容易含有病毒或是非法之盜版軟體，容易遭到廠商追蹤舉發而產生訴訟與巨額賠償。

七、全台近千網站植入惡意程式（一）

案由：

據媒體報導：平均每10個網頁，就有1個被植入惡意程式碼，「拒絕壞程式基金會」(http://stopbadware.org)發布「全台近千網站植入惡意程式」訊息，顯示目前網站內含惡意程式碼問題嚴重。

七、全台近千網站植入惡意程式(二)

預防方式：

(一)勿瀏覽非公務用途網站。

(二)個人電腦應安裝防毒軟體，作業系統及防毒軟體隨時更新。

(三)瀏覽器安全等級應設定為中級或更高等級。

(四)勿任意下載或安裝來路不明、有違反法令疑慮（如版權、智慧財產權等）的電腦軟體。

八、網路銀行資料遭竊取(一)

案由：（轉載自刑事警察局 ）

據科技犯罪防制中心指出：有犯罪集團利用假資料註冊與國內知名網路銀行、航空公司等極為類似之網址，再於各大搜尋引擎公司購買關鍵字廣告，誘使民眾連結至藏有木馬程式網頁，俟民眾電腦遭植入木馬後再導向正常網站，此時木馬程式已開始進行鍵盤側錄與竊取檔案，竊取民眾網路銀行帳號密碼，其後再進行轉帳盜取，此類損失達已數千萬元。

八、網路銀行資料遭竊取(二)

預防方式：

(一)使用搜尋引擎時需特別注意關鍵字廣告與正牌網站之區隔。

(二)個人電腦應安裝防毒與防火牆軟體，作業系統及防毒軟體應定期更新。

(三)避免將個人基本資料於網路上流傳。

(四)避免於辦公室瀏覽非公務網站。

九、涉國家安全研究領域教授之E-mail帳號遭盜用(一)

案由：

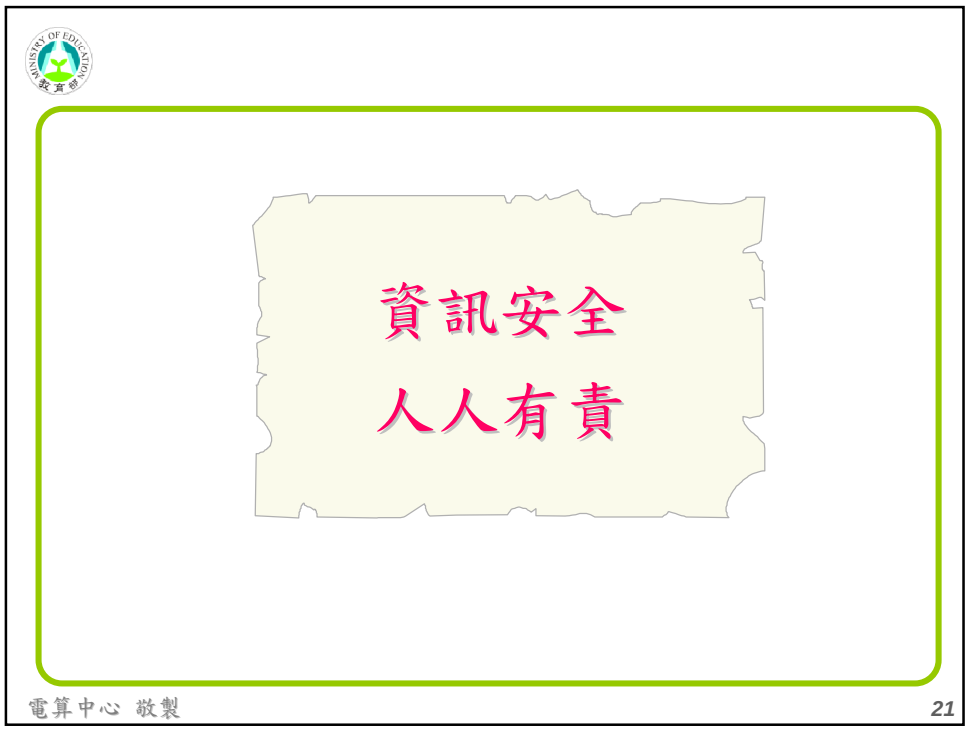
法務部調查局調查駭客中繼站發現某研究中共軍事、國家安全等領域教授，其E-mail帳號已遭竊取，追查來源為中國大陸。

九、涉國家安全研究領域教授之E-mail帳號遭盜用(二)

預防方式：

(一)針對校內承接政府計畫或學術研究涉國家安全、軍事機密等教職員、學生，各校應提醒及宣導該人員應特別注意資通安全，並協助其資訊安全防護。

(二)機密性、敏感性資料應妥善處理，不可置於公開網路上或使用E-mail傳遞。


資訊安全
人人有責
電算中心 敬製
21