2017年
個資保護及資訊安全
教育訓練

主講：陳冠宇

2017-09-25

我們公司的認證

- BS10012:2009 個人資訊管理系統
- 於 2016-12-19 通過複評驗證。
  有效期限：2014-01-08~2020-01-07
- 今年續評日期預定為11/23

- 品質 是我們一貫的堅持
- 專業 是我們服務的基礎
- 誠懇 是我們處事的態度
- 安全 是我們事業的保障

資訊安全政策

個人資料保護要求

- 遵守中華民國個人資料保護法及其相關法律法規要求。
- 遵守公司個人資料保護要求。
- 保護受託客戶之資訊安全及遵守個人資料管理要求。

對於資訊安全及個人資料蒐集、處理及利用，因執行業務所持有之任何個人資料，負有保密義務，非經公司同意，不得以任何方式，直接或間接向第三人透露或使其知悉。

- 蒐集：依法進行告知義務 / 取得同意。
- 處理：採取適當的保護措施，
  避免個人資料被竊取、竄改或毀損。
- 利用：應於蒐集之特定目的內使用，
  特定目的外之使用應另外取得書面同意。
- 傳遞：傳遞及交換分享中採取適當的保護措施，
  避免個人資料被竊取、竄改或毀損。
- 銷毀：特定目的消失 / 期限屆滿 / 當事人要求。

個人資料 生命週期

新版個資法修法重點

104年12月30日修正公布之「個人資料保護法」部分條文，經行政院發布於105年03月15日施行。

- 將病歷納入特種個資，可明確本條適用之範圍，與需要特別管理之對象。
- 放寬事業於蒐集、處理或利用特種個人資料之限制，以加強個人資料之合理利用，如允許經當事人書面同意後即得蒐集其特種個資。
- 對於一般個資的蒐集，放寬當事人除了書面以外的表達方式，不再侷限於書面方式。

資料安全控管

- 檔案軌跡 LOG 紀錄 (檔案傳輸、刪除)
- 電腦、系統帳號權限（檔案存取）
- 個人電腦與文件（密碼鎖定、桌面清空）
- 門禁權限與管制（設備維護、進出貨、訪客）
- 物料銷毀（待銷毀品管控）
- 管理作業程序 (管理、更新與執行)

資訊安全目標

資訊安全的目標是維護資料的

- 機密性-確保資訊隱密性並避免遭到非法存取
- 完整性-確保可提供正確與完整的資訊
- 可用性-確保可適時提供可用及正確之資訊

關於勒索病毒軟體

- 勒索軟體（Ransomware）又名流氓軟體
- 會針對目標檔案使用加密演算法進行加密，多為文件與影音照片，讓使用者無法開啟自己的檔案，由於文件與影音照片對大部分使用者的價值較高，所以願意付出贖金的意願也會更大。
- 然後在電腦中留下聯繫方式（如下張畫面），要求受害者交付贖金，才能取得將檔案解密的解密金鑰。


Ooops, your files have been encrypted!
Chinese (traditiona
我的電腦出了什麼問題？
您的一些重要文件被我加密保存了。
照片、圖片、文檔、壓縮包、音頻、視頻文件、exe文件等，幾乎所有類型的文件都被加密了，因此不能正常打開。
這和一般文件損壞有本質上的區別。您大可在網上找找恢復文件的方法，我敢保證，沒有我們的解密服務，就算老天爺來了也不能恢復這些文檔。
有沒有恢復這些文檔的方法？
當然有可恢復的方法。只能通過我們的解密服務才能恢復。我以人格擔保，能夠提供安全有效的恢復服務。
但這是收費的，也不能無限期的推遲。
請點擊 <Decrypt> 按鈕，就可以免費恢復一些文檔。請您放心，我是絕不會騙你的。
但想要恢復全部文檔，需要付款點費用。
是否隨時都可以固定金額付款，就會恢復的嗎，當然不是，推遲付款時間越長對你不利。
最好3天之內付款費用，過了三天費用就會翻倍。
還有，一個禮拜之內未付款，將會永遠恢復不了。
對了，忘了告訴你，對半年以上沒錢付款的窮人，會有活動免費恢復，能否輪
Payment will be raised on
1/4/1970 08:00:00
Time Left
00:00:00:00
Your files will be lost on
1/8/1970 08:00:00
Time Left
00:00:00:00
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $600 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Copy
Check Payment
Decrypt

勒索軟體的感染途徑

- 社交工程郵件（釣魚郵件寄送附件或有害連結）
- 軟體漏洞造成（網頁掛馬、惡意廣告程式）
- 內含惡意程式網路廣告
- 被駭客入侵的網站
- 內含惡意程式論壇文章
- 勒索軟體感染過程
  多數加密勒索病毒執行過程，一般都會向遠端遙控C&C主機取得加密金鑰，再暗中加密受害電腦中的檔案，如先使用AES加密檔案，再用非對稱金鑰RSA加密來將AES金鑰加密，且金鑰長度是2048位元，使用戶難以用暴力方式解開加密。

勒索軟體的處置原則

- 中斷網路連線
- 即刻發現，應立馬關機
- 評估災情
- 系統重灌，但軟體防護要更注意
- 保存現場狀況，請求支援
- 沒有辦法中的辦法（不建議）：付贖金

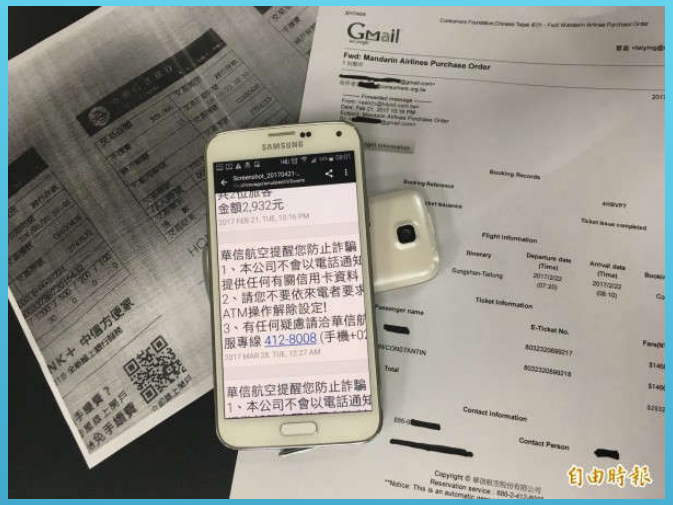
如何防範勒索軟體

- 不要打開未確認的郵件或點入它們內嵌的連結，那可能會開始安裝勒索軟體。
- 採用3-2-1規則來備份你的重要檔案：在兩種不同媒介上建立三個備份，其中一個備份要放在不同的地方。
- 定期更新軟體、程式和應用程式以確保其維持在最新狀態，可以防範新的漏洞。

2017-01-11

台北市資訊局「薪資發放管理系統」發生資料外洩情形，7萬多名北市各級公務員姓名、薪資、帳號敏感個資外洩在網路上。

資安案例 - 個資外洩



2017-04-24

陳小姐於2月21日在華信航空網站購買2張台北至台東單程機票，刷卡支付2,932元後，於3月23日下午接到自稱是華信客服的來電，在確定姓名、電話、購買商品、金額、搭機班次、購買日期、email...等資料都正確後，要求至ATM操作解除分期付款，陳小姐不疑有他共匯出15筆款項，受騙金額共52萬元。

消基會董事長游開雄指出，陳小姐驚覺自己被詐騙後就聯絡華信航空，但航空公司卻聲稱自己也是受害者，並強調公司人員無洩漏旅客個資，且公司網站也無安全問題等，直到15天後才收到華信航空的警示簡訊；期間不只造成更多的消費者受害，也延誤了防堵詐騙的黃金時間，依照個資法規定，陳小姐除了可要求業者賠償500元以上，2萬元以下金額外，亦可要求其賠償受騙金額。

資安案例-個資外洩

2017-05-10

空軍新竹基地張姓上尉參謀官因沉迷樂透彩，積欠12家地下錢莊超過100萬元，居然將基地官兵約400人的姓名與手機等個資，交給錢莊當作抵押，錢莊事後打電話進基地揚言「握有基地官兵的個資！叫張男快還錢！」全案才爆發，新竹檢方上週依個人資料保護法起訴張姓上尉。

資安案例-個資外洩

2017-05-12

台中檢調破獲史上最大宗個資外洩案！梁兆德個資蟑螂集團，涉從不詳管道取得全台一億七千萬筆全民個資，製成「客戶開發搜尋系統」販售給房仲，房仲可透過系統內建的駭客程式連線到地政機關，破解並海量比對，查出單一地主、屋主個資，包括總統蔡英文、首富郭台銘與天后蔡依林的個資，應也在內，檢調搜索帶回主嫌梁兆德、蘇慶典與房仲買家等六十二人，昨依違反《個人資料保護法》將蘇男、梁男聲押獲准，並續查資料外洩來源。

資安案例 - 個資外洩

2017-06-20

美國史上最嚴重！近2億選民個資慘遭外洩！美國資安研究人員證實，一家為共和黨全國委員會和其他共和黨人士服務的資料分析公司「深根（Deep Root）」，疑似在一次更新時不小心解除檔案的加密保護，把1.1ＴＢ檔案，包括約佔62%美國人口的1.98億選民姓名、生日、住家地址、電話號碼等個資，暴露在公開的網路世界十二天，期間任何人都能輕易下載這些資料。該起事件據信為史上最大宗的美國選民資料外洩案。

資安案例-個資外洩

違反個資法的罰則

民事責任	對於不易或不能證明實際損害額時，規定每人每一事件可求償5百元以上2萬元以下，而同一事件的最高賠償總額為2億元以下。
刑事責任	最高可處2年以下有期徒刑、拘役或科或併科新臺幣20萬元以下罰金。 對於意圖營利而犯罪者，特別加重罰責，最高可處5年以下有期徒刑，得併科新臺幣100萬元以下罰金。
行政處罰	最高可處新臺幣5萬元以上50萬元以下罰鍰並可限期改善，若未改善可繼續處罰。

簡報結束

請記得簽名並繳回試券

謝謝！