成大資通安全研發中心
INFORMATION & COMMUNICATION SECURITY RESEARCH AND DEVELOPMENT CENTER NCKU

資訊安全與個資保護

成大資通安全研發中心
鍾沛原 專案經理

Outline

- 網站安全與威脅現況
- 個人資安責任與防護
- 個人資料保護
- 結論

成大資通安全研發中心
INFORMATION & COMMUNICATION SECURITY RESEARCH AND DEVELOPMENT CENTER NCKU

網站安全與威脅現況

Cryptology and Network Security Laboratory, Institute of CCE, NCKU

網路安全事件層出不窮

美大學遭駭客入侵 30萬筆師生資料外洩

作者：編輯部 -10/15/2012

西北佛羅里達州立學院(NWFSC，Northwest Florida State College)日前證實，將近30萬筆學生、教職員的資料遭到駭客竊取，被竊資料除了個人基本資料外，也包含銀行與帳號等財務資訊。

NWFSC於10/8對外表示，3,200位現任與退休的員工個人資料被竊，被竊的資料包括姓名、生日、社會安全密碼，以及存款銀行與帳戶號碼…等，在進一步調查後，NWFSC發現問題比原先預估的更加嚴重，於是10/10再度公布，約7.6萬名仍在學與畢業學生的個人身分資訊遭竊取，另外，全佛羅里達州內，至少20萬名有資格申請「光明前途(Bright Futures)」獎學金的學生資料，包括姓名、社會安全號碼、生日、種族和性別等也遭竊取。

繼10月初傳出全球數十所大學遭駭客攻擊，因而導致120萬筆學生資料外洩後，不到一個

資料來源：資安人

網路安全事件層出不窮(cont.)

Microsoft發出IE 9安全漏洞公告 承諾盡快釋出修補程式

曹乙帆 / 編譯 – 2012/09/19
分類： 安全防護, 新聞

16 | 1 | 2
讚 | Tweet | +1

微軟承諾會盡快釋出針對IE9及早先IE版本的零日攻擊漏洞修補程式，以避免使用者誤入惡意網站的風險。

微軟已收到基於IE9或早先版本之「少量鎖定式攻擊」的報告，同時該公司已對外發表安全公告，以協助消減被入侵的風險。

安全研究人員Eric Romang已確認出Nitro駭客團體所採用伺服器上的入侵碼，並認定已用來發動運用上個月報導之Java零日攻擊弱點的漏洞攻擊。

針對IE9零日漏洞，微軟已對外發表安全公告，以協助降低被入侵的風險。(圖片來源：http://technet.microsoft.com/en-us/security/advisory/2757760)

微軟可信賴運算事業群(Trustworthy Computing Group, TCG)總監Yunsun Wee指出，目前安全修補程式正著手開發之中，微軟用戶也可另外部署EMET(Enhanced Mitigation Experience

http://news.networkmagazine.com.tw/classification/security/2012/09/19/42107/

網路安全事件層出不窮(cont.)

2011年6月：過去兩個月來，先後「駭」了美國中央情報局（ＣＩＡ）、聯邦參議院等網站的駭客團體Lulz Security（簡稱LulzSec），二十五日突然宣布結束網路攻擊行動、組織解散，據信原因與執法單位和競爭對手駭客都在追查這個駭客團體有關。該團體十九歲成員克萊利本週在英國被捕。

花旗也被駭 270萬美元飛了

REUTERS 更新日期：2011/06/29 09:36

（路透華盛頓28日電）「華爾街日報」（WallStreet Journal）報導，按資產計算美國第3大銀行花旗集團告訴政府官員，約3400名客戶信用卡資料被駭，損失金額達270萬美元。

但花旗集團表示，客戶無需為「任何未經授權使用他們帳戶所導致的損失負責」。

您已於 2011/5/13 下午 04:51 轉寄這封郵件。

寄件者: 玉山銀行網路服務 <Netbankservice@esunbank.com.tw>
收件者: Undisclosed-Recipient:;
副本:
主旨: 玉山網路銀行-轉入款項通知

訊息 轉帳通知明細.rar

您好，
此為透過玉山網路銀行完成以下交易之訊息回報，敬請參考。
・交易類別：即時轉帳通知
・交易時間：2011/05/13 下午 14:46:00
・轉入帳號：808/0749xxxxxx068
・轉帳金額：NT$106,000.00
・轉帳摘要：
・附註：本訊息為轉帳人透過玉山網路銀行通知您，請向您的帳戶所屬

玉山網路

※本資料僅供參考，實際交易結果以本行系統為準
※請勿直接回覆此信，若有疑問請至本行網站訪客留言版留言，我們將

轉帳通知明細.rar - RAR 壓縮檔, 未封裝大小 423,424 位元組

名稱

..

轉帳通知明細.rcs.doc

寄件者: may-06573@email.esunbank.com.tw
收件者: Undisclosed-Recipient:;
副本:
主旨: 20110629重點新聞摘要!..祝投資順利~~

訊息 20110629重點新聞摘要.rar (132 KB)

寄件者: 慈濟學會 <ciji_server@msa.hinet.net>
收件者: Undisclosed-Recipient:;
副本:
主旨: 慈濟素食譜-養生篇

訊息 慈濟素食譜-養生篇.rar

> 慈濟素食譜-養生篇
>
> 三杯麻油菇
>
>
>
> 材料：
>
> 調味料：
>
> 老薑、杏鮑菇、珊瑚菇、鮑魚菇、九層塔
>
> 麻油、糖、素沙茶醬、蠔油
>
>
>
>
>
> 作法：
>
> 1. 老薑切片，菇類切小塊，薑片於油鍋內爆香備用。
> 2. 將菇類全部川燙後泡冷水再將水分擠乾，油炸備用。

【每日小語：脾氣慢半拍．吵嘴一回合．見面三句話．交談要微笑．佛光菜根譚】

☆以下內容由各投資機構提供，爲純屬研究性質，僅供參考。使用者應明瞭其參考

【 台灣股市－主要指數 】

指數名稱	最新指數	漲跌	漲跌幅	成交金額
加權指釋	8788.40	61.31	0.70%	871.78 億
櫃買指數	136.81	1.64	1.21%	200.55 億

法人	外資	投信	自營商
買賣金額	-21.82 億	5.20 億	9.48 億

寄件者: 中華電信電子帳單 <cht_ebpp@cht.com.tw>

收件者: Undisclosed-Recipient:;

副本:

主旨: 中華電信100年5月電信費用通知單[郵件編號:101684319]

訊息 4207721_10005_notification.pdf (189 KB)

中華電信 電子帳單 e-Bill

親愛的 客戶，您好： 使用注意事項 意見反映請按此 **[本信件為系統自動發送,請勿直接回信]**

請輸入密碼開啟附加檔案瀏覽您本期的電子帳單（密碼即『身份證號』**(第一碼英文字母須大寫)**，營業人客戶不需輸入密碼，直接點選附加檔案，即可瀏覽），如您要線上繳費或使用其他服務，請進入電子帳單點選 [我的電子帳單e-Bill] 選項。

若您有任何疑問，歡迎您隨時電洽本公司免付費服務電話：123(行動電話請撥：0800-080090)。

e-Bill ▸▸Hot

重要訊息公告

1、自100年1月起，本公司月租費與通信費計費期間調整一致，請參閱帳單上說明。(NEW!)

2、中華電信與Yahoo!奇摩合作電子帳單專送服務，貴客戶申辦電子帳單，除可使用本公司HiNet信箱，亦歡迎選用Yahoo!奇摩電子信箱。

3、貴客戶如接到公務機關或金融單位來電顯示之代表號或0800免費服務號碼時，請勿相信以免受騙並立即通知165反詐騙專線。

4、自97年4月起，行動電話客戶可利用GPRS手機隨時隨地上網瀏覽電子帳單及繳費，詳情請參閱「電子帳單問答集」(http://www.cht.com.tw/ou_web/chtn/ebill/index.htm)。

5、小心提防「詐騙電話」：中華電信語音通告絕無請您按任何號碼轉接客服人員，接獲可疑來電切勿回應，請先掛斷電話，再撥165反詐騙專線查證。

好康報你知 ▸▸New

分析這些現象...

- 人人都知道資安很重要，但卻不知如何做
  - 舊的威脅依然存在。
  - 錯誤的觀念，將駭客拱成英雄。
  - 犯罪者利用來進行犯罪行為。
- 駭客攻擊的手法趨於多樣化及混和型的攻擊
  - 竊取機敏資料
  - 從中獲取利益$$
- 使用者已成為主要攻擊對象
- 隨身資訊設備將是下一波散播惡意程式的媒介

駭客攻擊後 索尼將恢復網路服務

AFP 更新日期：2011/05/15 13:50

（法新社東京15日電）索尼公司（Sony）表示，他們今天將開始分階段恢復網路服務。索尼的網路服務先前遭駭客攻擊，外洩的資料量在網路史上數一數二。

索尼最近數週遭遇多次網路攻擊，涉及使用PlayStation Network與Sony Online Entertainment服務的逾1億個帳號，這些使用者的名字、密碼與電郵地址等個資遭竊。

索尼說，無法排除數百萬個信用卡號碼也有被竊危險。1

成大資通安全研發中心
INFORMATION & COMMUNICATION SECURITY RESEARCH AND DEVELOPMENT CENTER NCKU

個人資安責任與防護

Cryptology and Network Security Laboratory, Institute of CCE, NCKU

一般使用者的迷思

- 茫茫網海使用者何其多，怎麼可能那麼倒楣駭客一定找上我？
  駭客可以利用自動化工具亂槍打鳥，也會瞄準特定目標進行攻擊

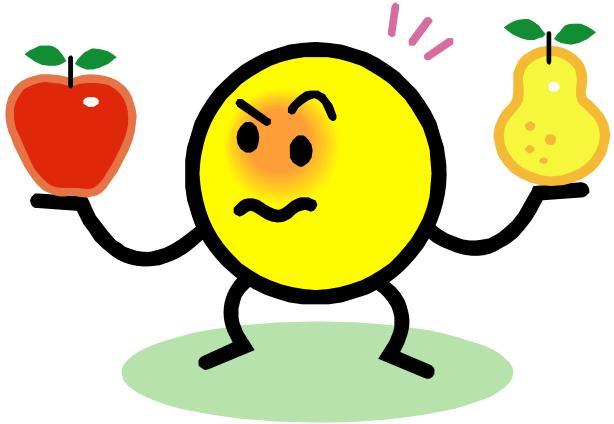
- 我只要不亂開啟來路不明的mail與檔案，也不瀏覽奇怪的網站，就都安全了！
  駭客會假冒使用者信賴的帳號，發送經偽裝的惡意檔案，並誘使點擊假造的可信賴網站，甚至針對該網站之漏洞發動攻擊！

- 只要安裝防毒軟體，定期更新病毒檔以及軟體修補程式，就不會被駭客攻擊了！
  在醫學界，先有「病毒」才有「疫苗」！同理可證，在大部分的情況，駭客發展出新型態的攻擊手法，資安研究組織才知道該如何進行防護！

那我到底該怎麼辦！？

治標的方法：養成良好的使用習慣

OR



治本的方法：這輩子不再使用網路

個人資安責任

- 密碼管理
- 設備管理
- 桌面、螢幕淨空管理
- 電子郵件管理
- 即時通訊管理
- 個人資安觀念

密碼管理

- 帳號/密碼的組合，是最常用的身分驗證機制，亦是駭客最常攻擊的部分
- 定期更新密碼。
- 不使用弱密碼
- 不寫下密碼。
- 不提供密碼予他人。
- 有洩漏的懷疑即更換密碼

安全的個人密碼設定

- 您的密碼不應該包含：
  - 生日組合(601023)
  - 太短或英文單字(hsiuping)
  - 家人、情人、寵物的名字
  - 倒著打(gnipuish)
  - 出現頻率太高(0000)或太連續(abc123)
  - 一組密碼行遍天下

安全的個人密碼設定(cont.)

- 您的密碼應該要：
  - 大小寫英文、符號、數字混合(I'mGaY@5438)
  - 長度足夠，建議六個字元以上
  - 使用國語或台語拼音，組合成較長且無英文字義的字母串，卻又容易記憶。例如「warDerMeeMar」(我的密碼)。
  - 不要使用自己的基本資料當密碼，例如：出生日期、身份證字號、姓名。
  - 不要依英文及數字在鍵盤上的排列位置輸入密碼，例如：qwerty、asdfgh等。
  - 定期變更密碼(很難做到)
- 不在不安全的電腦(網咖、共用電腦)輸入密碼

有設定密碼就安全了嗎？

- 分析34,000筆自MySpace釣魚網站取得的使用者帳號和密碼資料：(Real-World Passwords,2006/12)

密碼數	比例
1-4	0.82%
5	1.1%
6	15%
7	23%
8	25%
9	17%
10	13%
11	2.7%
12	0.93%
13-32	0.93%

密碼組成	比例
數字	1.3%
字母5	9.6%
字母與數字混合	81%
非字母也非數字	8.3%

- 28%為小寫字體加上一個數字，其中2/3的數字是“1”。
- 3.8%是一完整單字。
- 12%是單字後加一個數字，其中2/3的數字是“1”。

Password Top 20

名次	Password	名次	Password	名次	Password	名次	Password
1	password1	6	Qwerty1	11	123456	16	jordan23
2	Abc123	7	fuckyou	12	soccer	17	slipkbot1
3	Myspace1	8	123abc	13	monkey1	18	superman1
4	Password	9	baseball1	14	liverpool1	19	Iloveyou1
5	blink182	10	football1	15	princess1	20	monkey

雙核心CPU電腦破解密碼時間統計表

密碼組合內容	破解時間	
	密碼長度六位	密碼長度八位
數字密碼 (10)	1秒以內	3分鐘
大小寫字母 (52)	33分鐘	62天
大小寫字母 + 數字 (62)	1.5小時	253天
大小寫字母 + 數字 + 符號 (96)	22小時	23年

本研究整理，資料來源：http://www.lockdown.co.uk (2006)

微軟的密碼強度檢查工具

- Password checker
  - https://www.microsoft.com/protect/yourself/password/checker.mspx

Geekwisdom密碼強度測量工具

- Javascript Password Strength Meter
  - http://www.geekwisdom.com/dyn/passwdmeter

設備管理

- 安裝防毒和防火牆軟體。
- 定期做好資料備份(公務上的需要)。
- 定期更新系統與軟體之修復檔(Path)。
- 不遺留機敏資料在印表機、掃瞄機、傳真機等設備。
- 不提供給他人使用。
- 不使用他人設備處理機敏資料。
- 養成關機的習慣。

桌面、螢幕淨空管理

- 機敏資料不隨意置放在桌面上。
- 設定螢幕保護程式(要設定密碼)。
- 離開座位或不使用螢幕時，要鎖定螢幕。

電子郵件管理

- 不隨意開啟來路不明郵件的附加檔案。
- 設定垃圾郵件過濾之規則。
- 使用垃圾郵件過濾軟體。
- 不回覆垃圾郵件。
- 不轉寄帶來好運或厄運的信件。
- 寄送機敏資料給多人時，可使用密件副本功能。
- 不寄送機敏資料給非相關人士。

電子郵件安全

- 利用現有的mail client弱點
  - Outlook/outlook express
- 夾帶檔案
  - 夾帶執行檔
  - Jpg.exe
  - Jpg……exe
- 夾藏在HTML格式中
  - Iframe
  - XSS..etc.,

電子郵件社交工程

- 多以e-Mail方式散布
- 常被包裝在一個「正常」的執行檔中
  - 算命、心理測驗
  - 遊戲、笑話
  - 圖片、影片
- 一執行便被安裝後門程式、木馬程式
- 惡意程式能取得您電腦的使用權、監聽網路傳輸、按鍵輸入

電子郵件社交工程(cont.)

- 開啟以下檔案時，必須特別注意：
  - *.com
  - *.exe
  - *.bat (批次檔)
  - *.vba (巨集)
  - *.pif (Windows Program Information File)
  - *.zip, *.rar (壓縮檔)
  - *.doc, *.xls, *.ppt (Office)
  - *.scr (螢幕保護程式)

電子郵件社交工程(cont.)

- 電子郵件社交工程防範
  - 注意可疑電子郵件之特徵
    - 過於聳動的主旨與緊急要求，以引誘收信人開啟信件及回覆。
    - 不正常的發信時間。
    - 來路不明之電子郵件或少往來對象之來信 。
    - 認識的人（同事或朋友）來信但主旨或內容與其習性不符。
    - 要求輸入私密資料送出。
    - 連結金融機構網址更改基本資料。
    - 假冒寄件者。
    - 垃圾郵件。
    - 含有惡意程式的附件。
    - 利用零時差攻擊。

電子郵件社交工程(cont.)

- 可疑電子郵件之自我保護措施
  - 關閉預覽窗格。
  - 非必要閱讀之郵件逕行刪除。
  - 設定為純文字讀取模式再開啟郵件閱讀。
  - 開啟郵件內含之超連結時先確認連線網址之網域名稱(Domain Name)是否足以識別？若為數字IP之網址勿輕易開啟。
  - 不隨意輸入資料送出，傳送私密資料時確認是否有啟動加密機制。
  - 分辨電子郵件的真偽。於該信件按滑鼠右建，點選【內容】->【詳細資料】(Outlook Express)或點選【郵件選項】(Outlook)確認發信者電子郵件帳號，惟發信者電子郵件帳號仍有被偽冒的機率，必要時直接與寄信者連絡確認是否來信。

電子郵件社交工程(cont.)

有朋友收到這樣的一封信詐騙的.....

今天收到這樣一封信,內容如下

寄件者: jcic@jcic.org.tw
日期: 2006年7月4日 下午 07:14
收件者: 21世紀行銷名單47
主旨: 金融信用卡中心提醒您

看似正常的帳號，但按回信時，收件者會是.com的帳號

親愛的信用卡用戶您好：

近用僞卡集團及詐騙集團盛行，且手法日益高明，
本金融聯合信用卡中心近來發現有數十萬筆信用卡出現異常
，特此本中心提醒各廣大用戶，請儘速致本中心網站驗證您
所使用的信用卡是否有出現異常，以保障您個人的權益遭受
不明的損失！！　　特此公告　　金融聯合信用卡中心

金融聯合信用卡中心

http://jcic.cngsh.com！

畫面如下！

寄件者: HEEACT-蕭方雯 [fangwen.heeact@gmail.com]　　寄件日期: 2010/8/24 (星期二) 下午 04:50
收件者: Undisclosed-Recipient:@msr24.hinet.net;
副本:
主旨: 【HEEACT】敬送99下系所評鑑評鑑委員行前說明會邀請函
附件: 99下-評鑑委員研習會邀請函Invitation.rar (81 KB)

名稱	大小
..	
99下-評鑑委員研習會邀請函Invitationexe.doc	139,264

99下-評鑑委員研習會邀請函Invitationexe.doc

各位委員鈞鑒：

首先感謝 鈞座同意擔任評鑑委員，至為感激，特函申謝。

99年度本會將接續辦理9所軍警校院系所評鑑與97年度大學校院　　員

暨評鑑委員遴聘要點」評鑑委員須參與本會評鑑講習後方得聘任之。　　際

運作情形，於99年度之評鑑委員研習會，將邀請國防軍警校院代表，

本會將於99年9月15日上午9時至12時假國立編譯館10樓國際會議廳舉辦「**99年度下半年度系所評鑑評鑑委員行前研習會**」，煩請 鈞座於百忙之中撥冗參與。專此函達，佇後佳音！

並請 鈞座請以**e-mai回傳附件**。敬頌

鈞安

財團法人高等教育評鑑中心基金會 敬上

財團法人高等教育評鑑中心基金會
訪評專員：蕭方雯
地址：台北市和平東路一段145號7樓(評鑑業務處)

即時通訊管理

- 不使用記錄密碼之功能。
- 不隨意存取他人傳輸之檔案。
- 不隨意點選他人傳送之網址。
- 避免於工作時使用。
- 不透露訊息或傳遞檔案給他人。
- 定期更新程式。

愛用網路的您，可能面對...

行為	方法	目的
上網找資料 聊聊天 收發e-mail 下載新的電影 加入社群會員	惡意程式: 病毒、木馬 入侵、破解	竊取資訊 與詐騙

上網安全 三不政策

- 不自行下載軟體程式
  - 如果要下載程式，請至官方網站。
  - 不要相信入口網站的下載資料。
  - 不要聽從網頁下載元件的指令。
- 不執行外部來源程式
  - 不要執行(開啟)電子郵件的附件檔案(exe,pif)。
  - 不要互相傳送電子郵件的可愛檔案(doc,xls,pps) 。
  - 不要自行安裝自己私帶的程式。
- 不隨意洩漏真實資料
  - 不要隨意填寫真實資料
  - 不要轉寄包含大量e-mail address的郵件。

個人資安觀念

- 遵守資訊安全政策與規定。
- 不在公眾場合洩漏機敏訊息與資料。
- 避免在網路上記錄個人資訊。
- 謹慎處理機敏資料。
- 定期接受資安訓練。
- 隨時留意各種資安訊息。
- 小心駭客就在你身邊。

成大資通安全研發中心
INFORMATION & COMMUNICATION SECURITY RESEARCH AND DEVELOPMENT CENTER NCKU

個人資料保護

個資洩漏案例

雅虎遇「駭」，官方確認超過40萬帳戶資訊洩漏

數位時代網站 | 撰文者：劉翰謙編譯　發表日期：2012-07-14

讚　46 人說這讚。趕快 Sign Up 來看看朋友對哪些內容按讚。　+1 6

屋漏偏逢連夜雨，拿來形容網路巨人雅虎的現況，的確有種無奈的貼切。

由前執行長Scott Thompson發起，針對Facebook的惡意專利訴訟，在其因被爆學歷造假而遭撤換後，接任臨時執行長的Ross Levinsohn，上週與社交龍頭達成的和解以及進一步的合作，說讓整個網路圈鬆了口氣也不為過。沒想到，上個風暴才剛落幕，今天雅虎又捲進更嚴重的災難—官方承認，因遭到駭客攻擊，估計有40萬組的email帳戶個資外洩。

聲稱是為「叫醒」負責保管這些個資的企業，並將這些帳戶資訊公諸線上的「犯案者」，是名為D33D Company的駭客組織。儘管這些資料很快就被下線，但已經在網路上引起軒然大波，因為乍看之下，雅虎雖然承擔了所有的「惡名」，但受害的也許不只是使用yahoo.com的使用者—因為許多人可能是以別家的email申請雅虎帳號。

http://www.bnext.com.tw/article/view/cid/0/id/23909

個資洩漏案例(cont.)

扯！教官陳情個資曝光　教育部判賠

TVBS 更新日期：2011/05/30 11:53

新北市一名趙姓退役教官，不滿教育部少發一天薪水，上網陳情；沒想到，教育部竟將這名教官的個人相關資料，刊登在網站上；陳情人認為隱私權嚴重遭侵害，請求國賠20萬，台北地院判決應賠償5千元，創下公務機關侵害隱私判賠的罕見案例。

不當使用個資 3公司遭罰

中央通訊社 中央社－2012年3月8日 下午8:09

字 +字

（中央社記者吳靜君台北8日電）金管會今天表示，遠雄人壽從第一保經、萬榮保經取得未經當事人同意的個資，進行電話行銷，共處3家公司或公司負責人新台幣130萬元罰鍰，且遠雄人壽停止電銷1個月。

行政院金融監督管理委員會表示，民眾接到遠雄人壽的電話行銷時，發現從來沒與遠雄人壽往來，不知為何會被行銷，因此向金管會檢舉。

經金管會調查，是民眾與第一保險經紀人公司買過保單，第一保經與萬榮保經是關係企業，所以萬榮公司輕易取得第一保經個資。同時，萬榮公司又與遠雄人壽有業務合作關係，遠雄人壽才取得第一保經、萬榮保經的客戶個資。

金管會表示，根據統計，受害的個資共有225筆。

金管會表示，根據電腦處理個人資料保護法、保險法及保險經紀人管理規則規定，各處第一保經、萬榮保經60萬元罰鍰、遠雄人壽負責人10萬元、並且遠雄人壽停止電話行銷業務1個月。1010308

個資法帶來的影響

- 提升全民意識，正視個人資料保護。
- 確立握有個人資料的組織、管理者必須善盡保護之責。
- 只要擁有個人資料，就有責任。

網站的公開性


單位網站
個資外洩時單位網站需承擔完全責任
公開區
保護區
個資外洩時單位網站需承擔部份責任
無心之過
惡意竊取
個資外洩
合法管道
➢單位責任
無刑責
無適當防護機制
非法管道
➢駭客入侵
有刑責

新舊法比較

差　異	電腦處理個人資料保護法	個人資料保護法
適用主體及申請執照	公務機關、八類行業及指定適用之團體或個人→**有執照制度**	公務機關及任何自然人、法人、團體→**廢止執照制度**
保護客體	限經**電腦處理**之個人資料	**任何形式**之個人資料
特種資料	無規定	規定**醫療等五種資料**原則不得蒐集、處理或利用
通知義務	僅規定公告機制，無規定通知義務	規定無論直接或間接蒐集個人資料均需告知當事人
書面同意	無特別規定	有特別規定，尤其是**目的外利用之書面同意**

參考資料來源：1.全國法規資料庫
2.http://www.epa.gov.tw/FileDownload/FileHandler.ashx?FLID=2722

新舊法比較(cont.)

差　異	電腦處理個人資料保護法	個人資料保護法
拒絕接受行銷權利	無特別規定	**首次行銷時應提供免費拒絕之方式並尊重其意思**
當事人查詢資料權利	查詢限制過於嚴格	**放寬限制查詢**之規定以保障當事人之權利
團體訴訟	無規定	符合規定之公益團體**可代替當事人提起團體訴訟**
刑罰規定	1. 僅處罰意圖營利侵害個人資料隱私權益者，刑期為2年以下 2. 罰金上限為4萬~5萬 3. 告訴乃論罪	1. 違反本法規定雖未意圖營利亦予處罰，刑期為2年以下；意圖營利者加重其刑為5年以下，且為公訴罪 2. 罰金上限為**20萬~100萬** 3. 公務員涉案，依法得**加重其刑二分之一**，最重可處七年半徒刑，與刑責已接近涉及貪瀆案。
民事損害賠償總額限制	每人每一事件新臺幣**二萬元以上十萬元以下**計算；負損害賠償責任者最高可賠償總額新台幣**2000萬元**	每人每一事件新臺幣**五百元以上二萬元以下**計算；負損害賠償責任者最高可賠償總額新台幣**2億元**

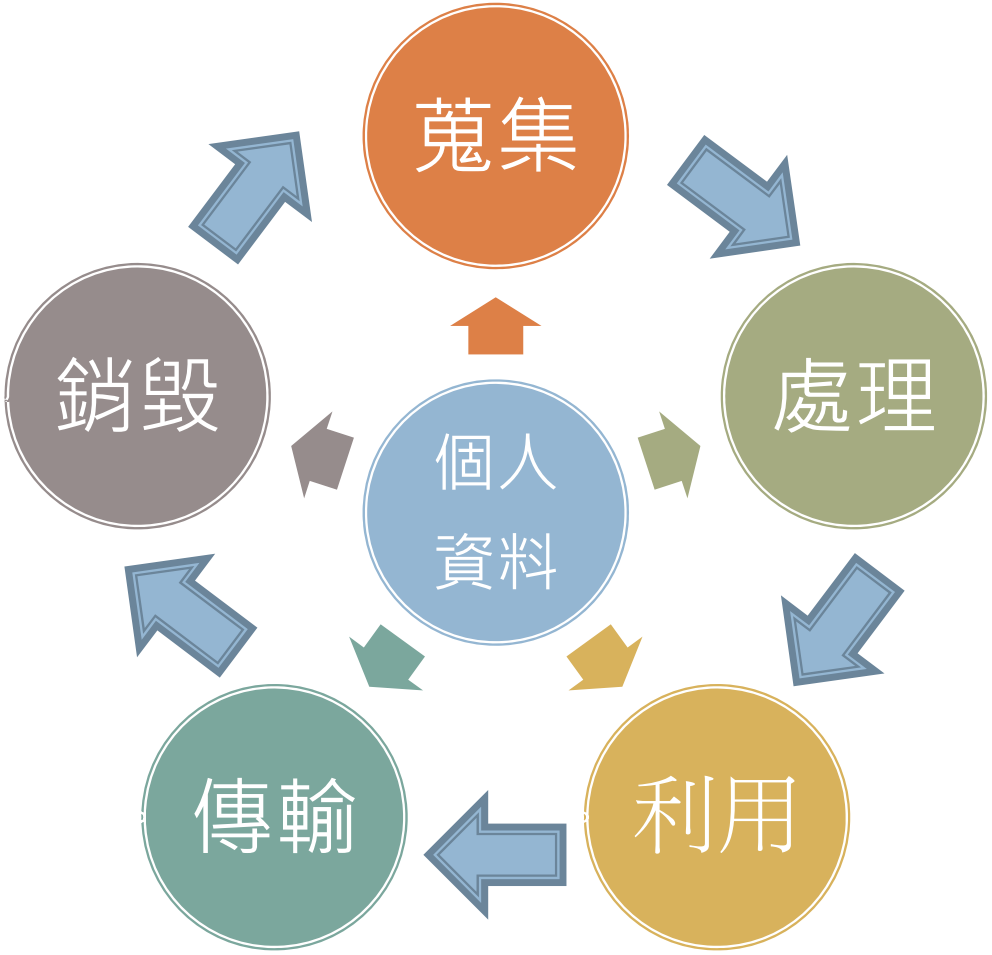
什麼是個人資料

- 個人資料保護法—第一章 總則

  第2條 本法用詞定義
  - 個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因 、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

    Q：姓名 + 出生年月日 + 身份證字號 = ?筆個資
  - 個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式 檢索、整理之個人資料之集合。

個人資料Life Cycle



當事人的基本權利

- 第3條
  - 當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：

    一、查詢或請求閱覽。

    二、請求製給複製本。

    三、請求補充或更正。

    四、請求停止蒐集、處理或利用。

    五、請求刪除。

    Q：如何證明已應使用者要求完成個資刪除？

- 第14條
  - 查詢或請求閱覽個人資料或製給複製本者，公務機關或非公務機關得酌收必要成本費用。

請求停止蒐集、處理或利用

銀行電銷擾民！　表明拒絕再打罰千萬

TVBS – 2012年3月28日 下午12:35

字 +字

相關內容

銀行電銷擾民！　表明拒絕再打罰千萬

銀行電銷擾民！　表明拒絕再打罰千萬

很多民眾一定都有接到電話行銷的經驗，有時候是銀行要推銷貸款，或者各種金融產品，常常一講就是一連串，掛都掛不掉，現在民眾不用怕整天被打擾了！金管會表示，只要民眾和銀行表明，不想再接到類似電話，銀行一週內要把不能再打的資料註明清楚，民眾如果再接到，就可以投訴金管會，銀行最高將被罰鍰1000萬元。

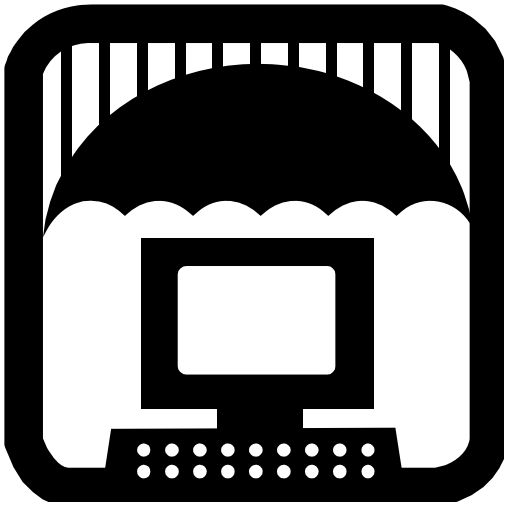
電銷人員：「先生不知道有沒有保險需要？」民眾：「不好意思，我在忙。」

銀行的行銷電話，有些人一天總要接上2、3通，而且掛都掛不掉。民眾：「跟他說現在在開會，很忙，他還是一直講，只好先掛。」

民眾：「什麼時候都有，有時候你正好在忙，我就跟他講說

不得逾越特定目的

- 第5條
  - 個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。



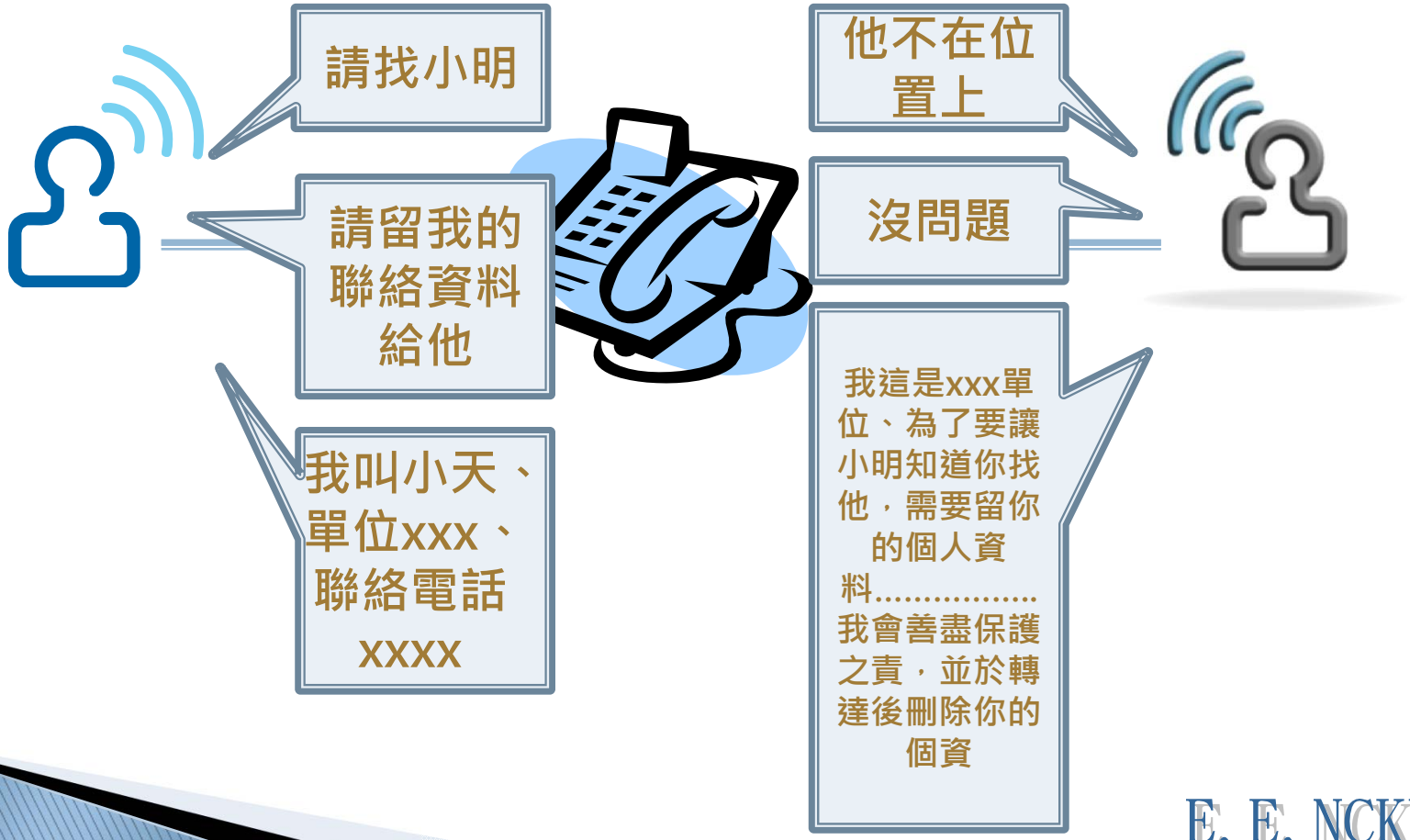
明確告知當事人事項

- 第8條
  - 公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：

    一、公務機關或非公務機關名稱。
    二、蒐集之目的。
    三、個人資料之類別。
    四、個人資料利用之期間、地區、對象及方式。
    五、當事人依第三條規定得行使之權利及方式。
    六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。

    有下列情形之一者，得免為前項之告知：
    一、依法律規定得免告知。
    二、個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。
    三、告知將妨害公務機關執行法定職務。
    四、告知將妨害第三人之重大利益。
    五、當事人明知應告知之內容。

以後打電話找人.....


請找小明
請留我的聯絡資料給他
我叫小天、單位xxx、聯絡電話xxxx
他不在位置上
沒問題
我這是xxx單位、為了要讓小明知道你找他，需要留你的個人資料.....我會善盡保護之責，並於轉達後刪除你的個資

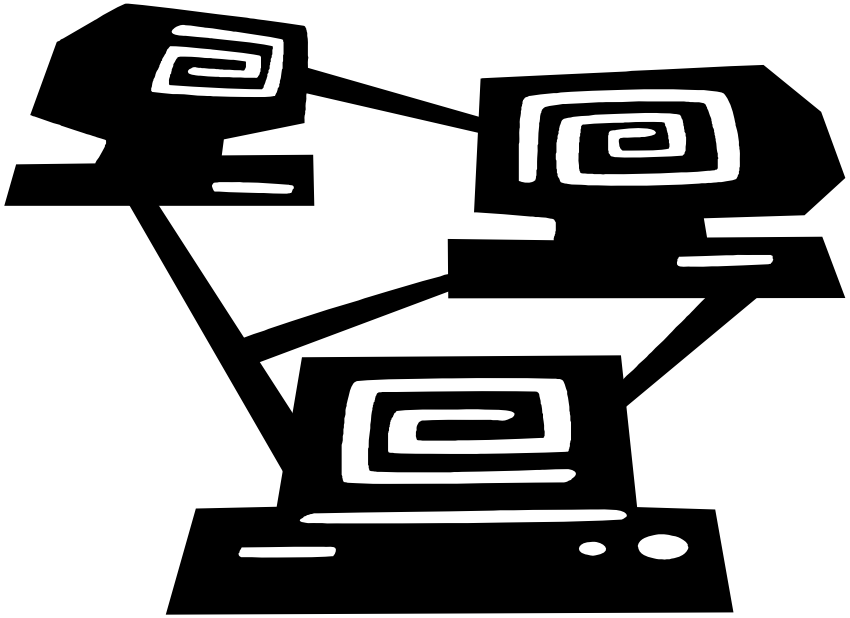

請找小明
請留我的聯絡資料給他
.....x#&@%
他不在位置上
嘟嘟.....

違反後的通知

- 第12條
  - 公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應**查明後以適當方式通知當事人**。

你的個資在哪裡？

- 家人
- 朋友、同學
- 學校
- 金融機構
- 電信業者
- 網路



你今天洩漏個資了嗎？

你能保護自己的個資嗎？

美面試趨勢 交出臉書密碼

中央通訊社 中央社 - 2012年3月24日 上午7:51

-字 +字

（中央社記者顏伶如波特蘭特稿）身為求職者的你，雇主面試時除了詢問基本資料，若還要求交出「臉書」帳號與密碼，你願意照辦嗎？越來越多美國民眾應徵工作時遇到這種困擾，公家機關尤其普遍。

近年來，隨著「臉書」（Facebook）日趨普遍，越來越多美國求職者現在找工作時，面試當中會碰到料想不到的「意外狀況」，就是雇主毫不避諱地要求應徵者告知「臉書」帳號及密碼。

網路科技的發達，讓現代人在網路上的一舉一動都將留下永恆足跡。位於社群網站龍頭老大地位的「臉書」，可以讓網友透過文字、照片分享各種生活點滴，如今也變成了雇主想要在最短時間內就能夠深入了解某位求職者的最簡便工具。

某些私人企業以及美國政府機構，則把利用「臉書」了解某位應徵者的做法更進一步「發揚光大」，不只是純粹瀏覽應徵者原本就公開分享的個人檔案與塗鴉牆內容，還要直接使用應徵者「臉書」的密碼登入帳號，仔細查看各種私密簡訊，原本設定不對外公開分享或

曝隱私更疏離 臉書在美退燒

作者：黃文正/綜合報導 | 中時電子報 – 2012年1月23日 下午4:41

-字 +字

中國時報【黃文正／綜合報導】

社群網站臉書（Facebook）風靡全球，擁有逾八億會員。不過，最近臉書在美國似已出現降溫現象，不僅越來越多年輕人拒絕加入，退出者也不在少數，對於這家亟欲提升市占率、準備明年風光上市的網路巨擘而言，恐怕不是好現象。

臉書在美雖有約二億會員，但成長已明顯趨緩。科技網站comScore數據顯示，今年一月至十月，瀏覽臉書的美國網友人數僅微增一○%，較去年同期驟減五六%。市調公司顧能（Gartner）分析師瓦爾德斯表示，臉書當務之急是如何提升現有廣大用戶的使用興趣，讓他們不斷回籠。

臉書一大賣點是與親友建立更親密的連結，但不少人卻認為，加入臉書反而讓他們感到更疏離。廿四歲的研究生艾爾瑟說：「我不再打電話給朋友，我只是查看更新，觀賞他們的

面對個資法，教育單位需思考...

- 如何建立全單位適用、能用的個資保護規範與流程？
- 如何分散個資保護的責任與風險？非單位需概括承受？非個人可置身事外？
- 商業行為不負擔教育顧客的責任，但教育顧客(學生)卻是教育單位的天責！

如何保護個資？

- 瞭解個資法
- 識別簽署的文件、勾核的聲明條款
- 不養成分享的習慣
- 適時的捍衛自己的權益

單機版個資掃瞄軟體

中華民國資料保護協會
Data Protection Association of R.O.C.

最新消息 | 協會簡介 | 服務項目 | 組織章程 | 聯絡我們

單機版個資檢測工具 (免費使用)

申請流程 | 系統規格 | 掃描步驟 | 商業版比較

申請流程

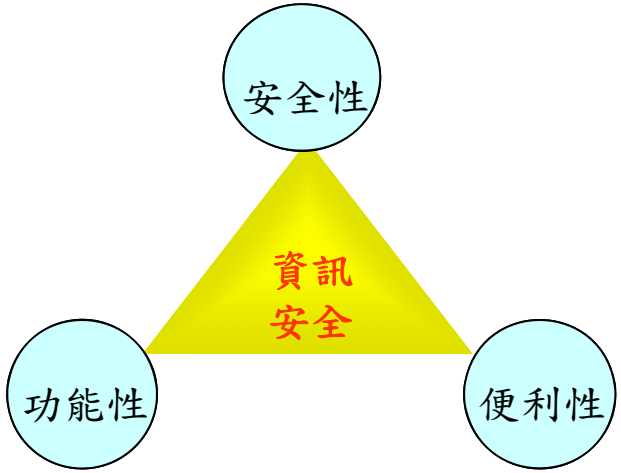
1.下載軟體(http://www.cdpa.org.tw/privacyagent.zip)
2.解壓縮後，點選privacyagent.exe
3.進入個資掃描步驟。
4.顯示個資掃描結果。
備註:本軟體僅供測試使用，如需商業使用，請與本協會聯繫(service@cdpa.org.tw)。

立即下載 | 資安人 INFO SECURITY 雜誌介紹內容

http://www.cdpa.org.tw/privacyagent.html

結論

- 資訊安全—
  - 說起來.....重要!
  - 做起來.....次要!!
  - 忙起來.....不要!!!
- 資通安全 = 技術+管理+稽核
  - 應達到“均衡”管理
  - “七分管理，二分技術，一分稽核”



Q&A