中華民國
臺灣警察專科學校
Taiwan police college

109年資訊安全教育訓練

講師：資安顧問 蘇江村

BCCS 漢昕科技股份有限公司
Business Continuity Computing System Inc.

1

課程大綱

- 資訊安全新聞案例宣導
- 要留意的五大資安威脅
- 社交工程簡介
- 電子郵件社交工程
- 日常作業的資訊安全

BCCS

2

資訊安全新聞案例宣導

BCCS 漢昕科技股份有限公司
Business Continuity Computing System Inc.

3

高市280名學童個資全都露 高雄市官員竟稱「被家長破解」

2020-01-16 12:14:47

[記者黃旭磊 / 高雄報導] 高雄市教育局公告實驗教育計畫錄取榜單，280名學童身分證字號等個資公告10個月後才移除，引發家長不滿，高市府教育局也挨批螺絲緊動。

人本教育文教基金會主任張萍、高雄市議員林于凱及律師曾友俞，今天對外說明洩漏事件；施姓小五家長到場表示，去年（2019）10月27日用google查閱「申請非學校型態實驗教育計畫」榜單，點選「**頁庫存檔**」模式開啟，竟發現孩子姓名、年級、身份證字號（以隱藏欄位處理）及設籍學校全都露，向主管科室反映才知為方便學生查詢才沒移除，從同年1月18日起公告已**事隔10個月**。

280名學童個資以EXCEL檔案格式上傳供查詢，資料於2019年11月移除；張萍指出，教育局不僅明顯有行政疏失，官員得知後怠慢不以為意，還向某教育團體解釋「是**被對電腦資料熟悉的人破解**」，嚴重違反個人資料保護法。對此，律師曾友俞解釋，局方對於學童之隱私權侵害顯有可歸責性，應依**個資法28條第1項**負擔損害賠償責任。

高市教育局回應，該份名單就像入學名單一樣公布，方便學生查詢，由於家長指洩個資，未來將不再公布，研擬正式發函到申請人設籍學校，再由學生自行向校方查詢。

施姓家長批評，網路犯罪非常多，教育局不擔心小朋友資料被盜用借貸、盜刷信用卡嗎？難道不應保障個資隱密嗎？

林于凱指出，教育局沒主動告知，竟怪家長「網站搜尋能力太強」，如果不要那麼強可能就不知道，而依**個資法法第28條規定，家長可進行民事求償500元到2萬元，甚至權益或財產受損最高可求償到2億元**。

資料來源：自由時報
https://news.ltn.com.tw/news/life/breakingnews/3042124

BCCS

4

內湖警副所長涉洩新冠肺炎確診患者行蹤 拔官記一大過

(2020/2/10)

- 內湖分局指出，派出所可查詢新冠肺炎確診病患個資，廖姓巡佐涉嫌在2、3天前查詢患者個資後，疑似**翻拍**派出所的肺炎專案勤務文件資料，傳送給林姓友人，林又將該資料傳予黃姓友人，輾轉流出至臉書及LINE群組。
- 廖涉嫌洩露的個資包含確診患者姓名，居住社區，及回國後行蹤等。廖姓巡佐懊悔稱，當時沒想那麼多，拍下照片，目的只是想要提醒家人注意疫情。
- 警方表示，廖員無故將公務機密資料洩漏予不相關之第三人，致生事端，依違反**刑法第132條公務員洩漏國防以外秘密罪**及**個人資料保護法第41條**函送士林地檢察署偵辦，另違反**傳染病防治法第10條**部分，亦同時函請台北市政府衛生局依權責裁罰。

資料來源：https://udn.com/news/story/7315/4334520

5

武漢肺炎》495確診者個資全外流！愛知縣道歉：人為疏失

2020-05-05 20:18:20〔即時新聞／綜合報導〕武漢肺炎疫情於日本情勢嚴峻，目前累積確診人數多達1萬5368人，死亡566人。今（5）日，**日本愛知縣**政府更新確診人數時，誤把病人個資上傳至官方網站，全縣495名確診病患個資流出，也引發民眾恐慌。

綜合媒體報導，愛知縣政府在今天上午9點30至10點15，**誤將縣內495名確診者的資料以excel文件檔案發布在官方網站**，文件中有396名患者姓名被公布，包括**住院地點、負責衛生所、入院出院日期及個人居住地與聯繫方式等**，病人隱私都被公諸於世，發布45分鐘後，相關人員接獲民眾電話詢問才發現，緊急撤除，然而頁面已有739次瀏覽紀錄。

愛知縣政府於官方上發布道歉訊息，表示誤將民眾個資放上是因為發布人員處理時沒有仔細檢查才會造成紕漏，對於這樣的疏失日後會更謹慎，也對患者及家屬深表歉意。

資料來源：自由時報
https://news.ltn.com.tw/news/world/breakingnews/3155821

6

零時差攻擊(zero-day attack)

- 所謂的零時差漏洞是指軟體、韌體或硬體設計當中已被公開揭露但廠商卻仍未修補的缺失、弱點或錯誤。或許，研究人員已經揭露這項漏洞，廠商及開發人員也已經知道這項缺失，但卻尚未正式釋出更新來修補這項漏洞。
- 零時差攻擊的成功與否還要看企業的「暴險空窗期」有多久，也就是從漏洞發現、到廠商釋出修補更新、再到企業完成部署的這段期間。即使是已知的漏洞，這段暴險空窗期依然可能很久，這有時是企業的修補管理政策使然，有時則是因為修補更新的開發有相當的難度。空窗期越長，駭客就越有機會發動攻擊或長期潛伏而不被發現。

7

中山大學驚傳師生電子郵件被監控長達3年 起因是駭客濫用Open WebMail漏洞

(2019/11/8)

- 這起事件被發現的原因，是有位政治學的教授收到該校主任秘書約談信件，察覺不尋常而進行通報，校方展開調查後，才驚覺是一起**埋伏已久**的攻擊事件。
- 他們於11月4日接獲通報，分析電子郵件系統的事件記錄後，發現他們遭受入侵的時間點，是**2016年12月**，換言之，該校電子郵件系統**被監控了接近3年之久**。

- 初步認為是透過跨網站指令碼攻擊（XSS）滲透，冒名寄信則是藉由跨網站請求偽造（CSRF）攻擊進行，針對Open WebMail系統的漏洞，中山大學已於今年7月防堵。

資料來源：https://www.ithome.com.tw/news/134105

8

8

總統府、立法院接連遭駭客攻擊 恐竊取機密 北檢分案偵辦

鉅亨網編輯陳于晴2020/05/21 11:10

- 繼日前總統府遭駭，導致內部文件變造外流，520當天又傳出立委及國會電腦收到假借府方名義的釣魚郵件，刑事局長黃明昭今(21)日指出，昨晚接獲府方報案，經查發現，郵件藏有惡意程式，一旦打開就會中毒，法務部已將近期駭客攻擊事件報請北檢指揮偵辦。
- 黃明昭說明，許多立委反應接到總統府發出的郵件，內容要求填寫相關個人資料，府方昨晚已向刑事局報案，經過漏夜鑑識後發現，郵件藏著惡意程式，立委、服務處及國會內部的電腦皆有收到釣魚文，一旦打開就會中毒，恐怕會被安裝木馬程式，竊取相關重要資訊，呼籲立委及相關員工絕對不要打開郵件。
- 黃明昭表示，刑事局初步掌握郵件埋藏惡意程式，但來源還在追查，至於有多少立委已經受害，也正在清查當中，外界關注是否與總統府日前遭駭有關，黃明昭強調，近期駭客攻擊的密度相當高，不排除任何可能，但仍要有足夠的證據來證明連結性。

資料來源：
https://news.cnyes.com/news/id/4480297

9

資訊安全宣導
從中油資安事件看勒索軟體

Waring for Ransomware

10

中油遭受勒索軟體攻擊，部分付款方式暫停使用

事件起源-109年5月4日中午左右,臺灣中油公司各加油站系統遭網路攻擊

根據蘋果日報的報導，從今天（5月4日）中午開始，傳出有不少臺灣中油的加油站停擺，許多加油站的電腦當機，甚至出現只剩下一座加油島可用，民眾只能使用現金與信用卡加油，造成大排長龍的情況。對此，臺灣中油於在下午3時透過經濟部網站發出新聞稿，表示他們因為資訊系統出現操作異常，調查後發現遭到網路攻擊，有部分的系統感染勒索軟體病毒，導致加油站部分付款機制受到影響，消費者無法使用儲值卡（捷利卡）和行動支付（中油Pay）。

資料來源:https://www.ithome.com.tw/news/137373
圖片來源:https://hk.xfastest.com/52279/ransomware-taiwan-gas-station/

11

何謂勒索軟體(病毒)

勒索軟體，駭客透過網路攻擊滲入組織內電腦進行綁架電腦或其檔案，並要脅支付贖金，若不付出贖金將面臨一連串損失……

勒索軟體大致可分為二類:

一類是鎖住被害者的電腦，要求被害者必須繳納贖金，才能拿回電腦的控制權。

另一類則是加密被害者電腦上的檔案，亦是要求被害者繳納贖金，才能拿到解密金鑰，以便解密檔案。

此次中油事件即是屬於電腦遭鎖住，致使加油站系統無法運作。

圖片來源:https://blog.trendmicro.com.tw/?cat=2266

12

感染源到底在哪?

勒索病毒是如何感染的呢?誰又是0號帶源者?

勒索病毒會偽裝成合法商用軟體被使用者下載與安裝後，進而取得電腦的控制權。大部分的勒索病毒感染途徑是**釣魚電子郵件**，當使用者不小心點選釣魚信件內的超連結，就會連結下載勒索病毒程式；或者是開啟釣魚郵件中的附夾檔案，附夾檔案本身就是惡意程式。這些惡意程式會利用電腦系統漏洞，進一步加密電腦內的各式檔案。

臺灣中油公司此次事件據悉測應是駭客已針對其相關系統**覬覦已久**，並可能透過社交工程方式對該公司進行相關滲透工作，並選定於當日中午人員午休最脆弱時段發起攻擊，並立即感染各加油站員工常用部分線上付款服務。

圖片來源:https://blog.trendmicro.com.tw/?cat=2266

13

如何防範勒索軟體(病毒)

預防勒索軟體「三不四要」口訣

三不要:

一不要：不要開啟未經確認的郵件與附件並關閉郵件預覽功能

二不要：不要點選可疑的網頁連結並關閉瀏覽器上的Flash、Active等元件

三不要：不要輕信中獎、優惠、折扣、贈送、免費等不實訊息字眼

四要:

一要：**要再三確認給予資訊者身分**，
例如：電子郵件的寄件者身分、檔案提供者

二要：**要確實安裝防禦軟體並定期更新**，
例如：防毒軟體、防火牆

三要：**要開啟自動更新作業系統修補程式**，
例如：Windows Update

四要：**要養成良好的備份習慣**，
例如：定期備份、多重備份、異機備份、異地備份

好奇害死貓!!
面對來路不明的電子郵件或未被安全認證的儲存媒體(如USB)、應用軟體.....
千萬不要、不要、不要去點兩下，因為會中毒、會中毒、會中毒!!

14

勒索病毒番外篇-勒索信件

除了可怕的勒索病毒外還有可惡的勒索信件

此類多會提供被害人曾使用過的帳號密碼或聯絡方式，攻擊者宣稱「透過惡意程式側錄了你的密碼」，並利用網路攝影機錄製了隱私畫面，**被害人需於若干小時內支付贖金(如特定Bitcoin)。若未支付贖金，就會向受害者的家人、朋友、同事或社群網站的聯絡人散布隱私**照片或影片。

處理方式 ：

- **遮蔽網路攝影機鏡頭**，避免遭到有心人士側錄。
- **電腦軟體應安裝修補程式**，避免產生漏洞。

資料(圖片)來源:https://isafe.moe.edu.tw/article/2241?user_type=4&topic=9

15

勒索病毒番外篇-勒索信件

勒索信件-**惡意程式攻擊**

屬於**典型的病毒信**，其**內容多是請收件者確認匯款收據等相關資訊**，**附檔**為ZIP或 RAR壓縮檔，若為Office檔案類型格式，**通常帶有惡意**巨集程式，若為PDF檔其中可能含有 JavaScript 攻擊腳本，有些附檔內則含有**病毒**或木馬**程式**等**執行檔**。

正確處理方式：

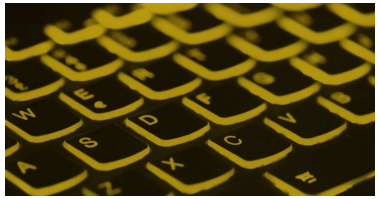
- **對來路不明的信件提高警覺**。
- **勿輕易開啟**未知**附檔**。

資料(圖片)來源:https://isafe.moe.edu.tw/article/2241?user_type=4&topic=9

16

橫行8年，曾名列臺灣十大網路威脅的惡意郵件殭屍網路Necurs巢穴遭剿清

- **多國民間與執法單位，聯手破獲Necurs組織用以散布垃圾郵件及惡意程式的基礎架構，阻止這個犯罪集團再度發動大規模攻擊**
- **文/林妍溱 | 2020-03-11發表**
- 微軟在取得紐約地方法院發布命令下，查獲Necurs用以散布垃圾郵件及惡意程式的基礎架構，使其背後的犯罪組織，無法再註冊新網域發動新攻擊。藉由分析Necurs以演算法產生新網域的技倆，微軟預測未來25個月內該犯罪組織可能註冊600多萬個網域，因此通報全球各國的網域註冊機關以封鎖這些惡意網站，使歹徒無法再註冊新網域。微軟同時也在多國ISP協助下，協助受Necurs感染的電腦清除惡意程式。
- 參與這次行動的，包括台灣、日本、西班牙、法國、波蘭、羅馬尼亞、印度、墨西哥、哥倫比亞等地的ISP、網域註冊機構、政府CERT及警方。



微軟表示，這次行動是經過8年的追蹤與策畫的成果。微軟的數位犯罪防治單位BitSight首先於2012年發現Necurs，散布的惡意程式包括GameOver Zeus銀行木馬程式等。Necurs受害者幾乎遍及全球各國，是全球最大的垃圾郵件殭屍網路之一，受感染電腦超過900萬台。微軟曾偵測到一台被Necurs感染的電腦在為期58天的調查期間，發送了380萬封垃圾郵件給4,060萬台電腦。Necurs也名列台灣2018年十大威脅來源之一。

資料來源：https://www.ithome.com.tw/news/136274

17

殭屍網路?

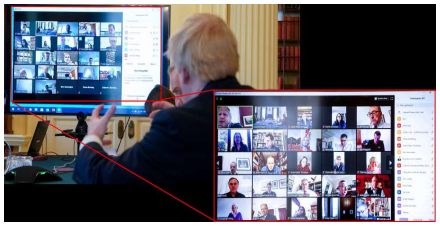
殭屍網路（botnet）是指感染殭屍網路病毒的被劫持電腦/設備所組成的網路，讓駭客可以進行遠端控制。殭屍網路被用來寄送垃圾郵件和進行分散式阻斷服務攻擊(DDoS)攻擊，並且也可以出租給其他網路犯罪分子。殭屍網路也可以在沒有命令和控制（C&C）伺服器的情況下存在，只要透過點對點（P2P）架構和其他管理通道來將命令從一台殭屍電腦（bot）傳到另一台。

18

Zoom接連爆發隱私與安全問題

文/羅正漢 | 2020-04-20發表

加拿大多倫多大學市民實驗室（Citizen Lab）的研究人員發布研究報告，為Zoom的不夠安全投下震撼彈。該報告指出三大重要發現，首先，是Zoom宣稱使用256位元的AES加密金鑰，但其實只有128位元，並且是較不理想的ECB模式；其次，是Zoom使用了上述非標準的加密方式，而且會議金鑰在特定情況會經中國伺服器產生與傳送；第三，則指出擔心Zoom會受制於中國政府的問題。



根據美國Cnet等媒體報導，美國參議院也要求所有的議員不要使用Zoom；而新加坡也傳出教育部要求教師暫停使用Zoom，根據當地媒體Channel News Asia報導，當地教育部在收到Zoom Bombing事件的報告後，為了預防起見，也要教師暫停使用Zoom，而在相隔4日後，才又允許逐步恢復使用。

資料來源：https://www.ithome.com.tw/news/137055

19

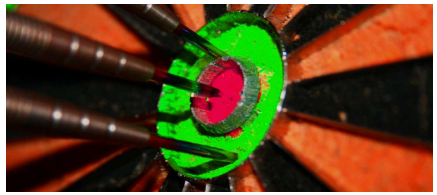
Zoom Bombing ?

- 在Zoom本身的多項隱私與資安漏洞之外，近期最多討論的安全問題就是Zoom Bombing，簡單來說，就是有其他使用者擅自闖入視訊會議的行為，並且故意在視訊畫面上分享色情或冒犯性的內容，干擾了會議的正常進行。
- 為何這些人能夠做出這樣的惡作劇行為？這事因為，他們可以找到公開在網路上的Zoom會議連結網址或會議ID，或是透過自動化工具找出有回應的會議ID。
- 對於如何不被外人闖入的問題，Zoom於官方部落格中，建議了3大使用原則。
- （一）要對螢幕的控制權有所掌握：在會議前或進行期間，設定自己是唯一可分享螢幕的成員
- （二）應做好與會者的管理：包括會議鎖定與刪除不需要的參與者等，而現在所有單一會議室主持人在召開會議時，需要強制設定密碼，用戶也應每次會議都設立不同的會議密碼
- （三）開啟等候室的功能：讓與會者不會立即進入會議，需要會議主持人一個個手動批准與會者進入會議室。

20

RDP暴力破解攻擊大幅增加

- 鑒於全球受到新型冠狀病毒(COVID-19)影響，現多數企業皆採居家辦公以因應全球疫情嚴峻局勢，因此增加企業網路安全隱憂。
- 依資安業者卡巴斯基(Kaspersky)觀察，從2020年3月中旬開始，透過暴力破解攻擊遠端桌面協定(Remote Desktop Protocol, RDP)之惡意活動大幅增加，受影響國家包括中國、義大利、美國、西班牙、德國、法國及俄羅斯等。以義大利為例，3月前每日相關攻擊次數皆低於15萬次，但3月中旬即竄升至50萬次，下旬更突破90萬次。而美國每日相關攻擊次數原本維持在20萬次，3月中旬即超越80萬次，4月更一度達到140萬次。



卡巴斯基研究人員表示，因使用者須從家中裝置連線至企業網路，然而許多RDP伺服器均有配置不良之問題，導致RDP暴力破解攻擊活動增加。卡巴斯基預估短期內相關攻擊活動不會趨緩，因此呼籲企業與使用者皆應採取防護措施，包括使用強密碼、啟用雙因子認證及規定只能經由企業虛擬網路(Virtual Private Network，VPN)存取RDP。另外，若無使用RDP之需求，則應關閉3389埠與相關功能，避免遭有心人士利用。為確保企業營運資料之機密性、可用性及完整性，在此關鍵時期企業更應做好健全準備，隨時備份所有重要資料。

資料來源：
https://www.ithome.com.tw/news/137357

21

1963年美援會搬遷 用牛車載運電腦

1963年9月，美援會改組為經合會，用牛車將辦公用的IBM電腦（打孔卡機）搬遷至台北市羅斯福路的新大樓裡，留下這幅「傳統支援科技」的經典畫面。

畫面中放置於牛車上的電腦由IBM製造，名為「打孔卡機」（Punched Card Machine，簡稱PCM），是一種用來對打孔卡片進行運算處理的機器，由於其內部組件經不起汽車運送時的劇烈震動，而在台灣又找不到具有良好避震設備的氣墊車，所以只好使用傳統的牛車，以時速5公里的安全速度，載著它緩緩地往目的地移動。

22

暴力破解法?

- 當攻擊者使用一組預定義值攻擊目標並分析響應直到他成功，這就叫做暴力攻擊。它的成功取決於預定義值的集合，如果它越大，就會需要更多時間，但成功的可能性也會變大。最常見且最容易理解的暴力攻擊是破解密碼的字典攻擊，在這種情況下，攻擊者使用包含數百萬個可作為密碼的單詞的密碼字典，然後攻擊者逐個嘗試這些密碼並進行身份驗證，如果字典中包含正確的密碼，攻擊者將會成功。

23

密碼怎麼設最安全又記得住？專家建議該這樣做！

文 / 記者黃敬淳 / 2020-02-25 08:24

- 儘管現代的網路瀏覽器、第三方密碼管理器或指紋辨識，都能便利地替用戶收納大量各方網站、網銀或網站服務的帳號密碼，不過無論如何，用戶至少都需要一個主密碼，才能獲得使用這些密碼的存取權。
- 而據 FBI 美國聯邦調查局每週技術專欄的建議，想設計一個安全的密碼，除了密碼長度至少得來到 15 個字符，與其使用一些複雜、看似亂碼的短詞，選擇幾組自己熟悉的單字和數字，再湊成一個長密碼，則是讓用戶自己可以記得住、同時又能有足夠安全性的重要原則。
- 例如，像「correct horse battery staple」這樣的密碼設計，便是一個不錯的選擇。將密碼的第一字換為英文大寫，或是將字母的「O」和數字的「0」錯位使用，並於整串英文密碼的最後綴上數字，也是不錯的設計。
- 挑選 4 個單字再組裝起來（每個詞之間可以再加入「-」符號）的密碼設計，也是今日安全的人員經常會建議用戶採用的方式。
- FBI 指出，因駭客不會知道用戶使用的單字，只要密碼長度拉長，攻擊者就需要花更多的時間與運算資源來破解。換言之，與其增加密碼構成的複雜度，增加密碼長度可能會是 CP 值更高的選擇。

特別的是，FBI 似乎對於使用「1Password」這類密碼管理器不是那麼認同，因這類管理器只要主密碼被破解，其他所有的密碼都會危在旦夕。

至於一些最差勁的密碼設計，據資安公司「SplashData」公佈的 2019 年選擇，仍以「123456」、「123456789」、「qwerty」和「password」這類粗糙的設計為主。

資料來源：
https://3c.ltn.com.tw/news/39623

24

密碼的安全設定原則

1. 不要使用懶人密碼
2. 長度與複雜度
3. 密碼不要有明顯的含義
4. 避免設定相同的密碼
5. 定期更新

25

密碼設定小撇步，善用技巧好記不糊塗！(1/2)

1. **穿插法**
   將兩個英文字或數字穿插，不過若使用兩組數字穿插可就沒有意義囉！
   - 範例：Good 與 2012 穿插後變成 G2o0o1d2
2. **字母位移法**
   將英文字母往前或往後移動幾個位置，如將 A 往後移動一位變成 B。
   - 範例：GOOD 往後移動一個字母變成 HPPE
3. **順序位移法**
   將英文字母往前或往後移動幾個位置，如將 A 往後移動一位變成 B。
   範例：GOOD 往後移動一個字母變成 HPPE
4. **鍵盤位移法**
   利用電腦鍵盤按鍵的位置進行字元移動，例如 A 向右移兩位為 D，B 向左移一位為 V。
   - 範例：將 GOOD 在鍵盤向左位移兩個字母變成 DUUA

26

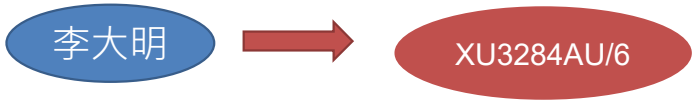
密碼設定小撇步，善用技巧好記不糊塗！(2/2)

5. **替換法**
   利用字形或發音相近的英文字母與數字交互替換，例如可以將英文字母 O 換成數字 0，字母 S 換成數字 5。
   - 範例：LOVE 替換後可變成L0V1
6. **輸入法變化**
   其實中文輸入法就是一種最簡單又有效的變換方式，只要把中文字的拼音轉換成鍵盤上的字母，簡單的密碼也可以變成難以猜測和理解的密碼囉！
   - 範例：將「大家好」使用注音輸入法成為 284 RU8 CL3。
7. **掐頭去尾法**
   利用喜歡的一段話（或一段歌詞），將其中每個英文單字的字首組合成密碼。
   - 範例：An Apple A Day Keeps The Doctor Away 取第一個字就是 AAADKTDA。

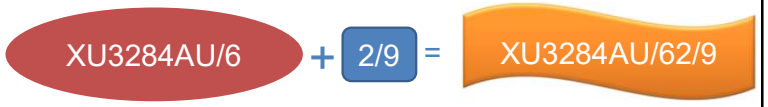
27

舉例：李大明 生日為 2/9

- 1.使用注音輸入法替換



- 2.加入生日日期 2/9



28

29

2019 年五大威脅

1. 家庭網路威脅：

我們的家庭越來越仰賴網路科技，有超過三分之二 (69%) 的美國家庭至少擁有一項智慧裝置：從具備語音助理功能的智慧喇叭、家庭保全系統到連網嬰兒監視器等等。然而安全上的漏洞，卻可能讓這些裝置成為駭客的鎖定目標，特別是擔任家庭網路進出閘道的路由器更是面臨重大危險。令人擔憂的是，83% 的路由器都含有可攻擊的資安漏洞。根據統計，光 2019 上半年就出現了大約 1.05 億次針對智慧家庭的攻擊。

BCCS

30

2019 年五大威脅

- **3.端點威脅：**

這是直接針對使用者而來的威脅，通常經由電子郵件散布。2019 上半年，趨勢科技偵測並攔截了超過 260 億次這類電子郵件威脅，約占所有網路威脅的 91%，這包括專為誘騙您點選資料或帳號登入憑證或者下載勒索病毒的網路釣惡意連結以竊取您個人魚攻擊。還有一些是透過幾可亂真的冒牌網站來誘騙您提供自己的個人資料。端點威脅有時也會使用社群媒體網路釣魚訊息，甚至是經由一些已經遭駭客植入惡意程式的正常網站來發動攻擊。

BCCS

31

2019 年五大威脅

- **3. 行動裝置威脅：**

駭客也會攻擊智慧型手機和平板，而且甚至更為積極。行動裝置使用者通常是在不知情的狀況下下載到惡意程式，因為它們會暗藏在一些看似正常的 Android 應用程式內，例如在全球感染超過 2,500 萬台手機的 Agent Smith 廣告程式。使用者除了超級容易遭到社群媒體攻擊之外，那些使用無安全性公共 Wi-Fi 網路上網的裝置也特別危險。不管駭客的手段為何，其目標就是為了賺錢：不論是竊取您的個人資料和登入憑證、大量顯示廣告、植入勒索病毒，或是強迫裝置撥打歹徒經營的高費率付費電話號碼等等。

BCCS

32

2019 年五大威脅

- **4. 網路帳戶已成為攻擊目標：**

  近來有越來越多駭客開始盯上使用者的帳號登入憑證，因為這是進入使用者數位生活的虛擬鑰匙。從 Netflix 到 Uber，從網頁郵件到網路銀行，這些帳號的登入憑證都能拿到黑暗網路地下市場上販售，或者用來蒐集個人身分資料。而針對個人的網路釣魚攻擊是取得這類帳號登入憑證的方式之一，不過 2019 年逐漸興起了另一種方式，那就是使用自動化工具來嘗試數萬筆帳號登入憑證是否套用到您的帳戶上。從 2017 年 11 月至 2019 年 3 月底為止，這類攻擊的偵測數量高達 550 億次。

33

2019 年五大威脅

- **5. 資料外洩無所不在：**

  能讓詐騙集團進入您網路帳號並且從事身分冒用詐騙所需的材料，都儲存在您網路帳號所屬的企業內。不幸的是，2019 年一再發生企業資料外洩的事件。截至 2019 年 11 月為止，美國有超過 1,200 起資料外洩事件，外洩的客戶資料筆數更高達 1.63 億。更糟糕的是，駭客現在還會竊取信用卡資料，他們會利用所謂的「數位盜卡」惡意程式，趁您在購物網站上輸入信用卡資料時直接加以盜取。

34

2020 年有哪些需要注意的事項?

- **1. 智慧家庭已成為攻擊目標：**
  - 當我們投資更多錢為家中添購更多智慧裝置時，請記住駭客也正加倍努力發動網路攻擊。因為有一項豐厚的報酬在向他們招手，那就是：利用某個暴露在外的智慧端點裝置入侵您的家用網路，進而蒐集您的個人資料和網路帳戶。或者，他們也可入侵您的保全攝影機來監控您家中情況，了解闖空門的最佳時機。此外，您被駭的裝置甚至可能被收編至殭屍網路當中，成為駭客攻擊他人的幫兇。

35

2020 年有哪些需要注意的事項?

- **2. 網路與電話社交工程攻擊：**
  - 專門利用使用者心理弱點的攻擊，一直以來都相當有效。相信 2020 年這類攻擊也不會缺席，不論是傳統的網路釣魚電子郵件，或是與日俱增的電話詐騙。美國民眾每天都會接到 2 億通「自動語音電話」，其中約 30% 是疑似詐騙電話。而且有時候電話詐騙也可能一轉眼就變成網路詐騙，例如那些刻意讓使用者以為自己的電腦出現問題的技術支援詐騙就是很好的例子。除此之外，歹徒也會利用社交工程技巧來詐騙錢財，例如，性愛勒索集團會宣稱他們手上握有受害者的性愛影片，並威脅要公開這些影片來要脅受害者。根據趨勢科技的偵測資料，這類攻擊從 2018 下半年至 2019 上半年成長了 319%

36

2020 年有哪些需要注意的事項?

- **3. 行動裝置威脅：**
  - 2020 年須小心行動裝置威脅將越來越猖狂。這當中有許多會來自於缺乏安全性的公共 Wi-Fi 網路，這類網路可讓駭客輕易暗中監視您上網的一舉一動並竊取您的身分資料和登入憑證。甚至一些公共的充電站都有可能遭人預先植入惡意程式，美國洛杉磯郡最近即發出這樣的警告。除此之外，別忘了還有惡意行動應用程式所帶來的威脅。

37

2020 年有哪些需要注意的事項?

- **4. 所有網路帳號都可能成為攻擊目標：**
  - 請注意，您今日開設並儲存了個人資料的任何網路帳號，明日都可能成為駭客攻擊的目標。當然，這意味著 2020 年您必須特別留意您的網路銀行帳號。此外，您還要小心針對遊戲帳號的攻擊。讓歹徒垂涎的不光只有您的個資和登入憑證而已，遊戲內的虛擬代幣也是歹徒豐厚獲利的來源。在所有偵測到的 550 億次登入憑證填充 (credential stuffing) 攻擊當中，有 120 億次鎖定的正是遊戲產業。

38

2020 年有哪些需要注意的事項?

- **5. 蠕蟲捲土重來：**
  - 電腦蠕蟲之所以危險，在於它們會不斷自我繁殖，這讓駭客不需自己動手，攻擊就能不斷擴大。2017 年 WannaCry 勒索病毒攻擊的情況就是如此。2020 年，一個外界稱為「BlueKeep」的 Microsoft 漏洞很可能會讓同樣的情況再度重演，而且未來可能還有更多像這樣的未爆彈。

39

40

社交工程介紹

- 組織常見的防護方式
  - **透過防火牆、IDS(網路防禦設備/軟體)與VPN(虛擬私有網路)等技術防範外部的攻擊**
  - **透過身分驗證機制等存取控制的手段來避免未經授權的存取**
  - **透過加密等方式來防範資料/檔案本身的隱密性**

上述增加防禦的縱深，我們稱之為階層式的防護

社交工程是透過「人」的弱點來達到入侵的目的

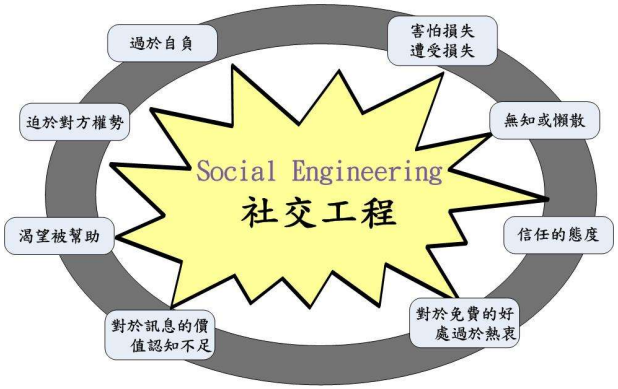
41

社交工程介紹(續)

- 社交工程是一種利用人類天性，透過嚴密的手段或騙局來得到敏感的資訊。通常利用人性的弱點不外乎下列幾種：
  - **對人的信任(人性本善)**
  - **恐懼的心態**
  - **渴望被幫助的需求**
- 社交工程通常想獲取下列的資訊
  - **授權或存取的詳細內容**
  - **敏感的資料**
  - **金錢或實質上的利益**

42

人性的弱點



43

社交工程的挑戰

- 社交工程是在安全上一個極為突出而且重要的威脅。主要的原因是社交工程被人們歸咎為羞辱而缺少相關的討論。
- 大多數的人們認為社交工程是在挑戰他們的智商與智慧，沒有人願意承認他們是社交工程的受害者。
- 因為這個事實，導致大多數的人將社交工程視為一個接近於禁忌的話題，而讓許多人還是容易受到社交工程的影響。

44

社交工程的類型

- 將社交工程的攻擊進行分類，大致上可歸為以下兩種類型：
  - **非技術性**

    利用欺騙/愚弄、模仿、暗中監視/偷聽、命令式口吻、假裝工作人員、假扮技術專家與Dumpster Diving
  - **技術性**

    Phishing、Vishing/Mishing、跳出的視窗、有趣的軟體、垃圾郵件

45

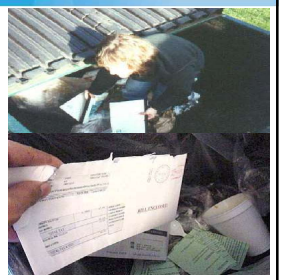
非技術性的社交工程方式

- **Pretexting/Impersonation 藉口/假扮(模仿)**
- **Spying and Eavesdropping 暗中觀察/偷聽**
- **Acting as a Technical Expert 假裝技術專家**
- **Support Staff 扮演工作人員**
- **Hoaxing 欺騙；愚弄**
- **Authoritative Voice 命令式的語氣**
- **Dumpster Diving 翻垃圾桶**

46

非技術性的社交工程方式

- 翻垃圾車(Dumpster Diving)
  - **由目標的公司要搜尋敏感資料，可以由：**
    - 垃圾桶。
    - 印表後廢棄的紙張。
    - 使用者的桌面上的便條紙、便利貼…等。
  - **可以搜集到：**
    - 電話/手機號碼。
    - 聯絡的資訊。
    - 財務的資訊。
    - 有關操作的資訊(如密碼、重要的文件存放位置…等)。
  - **案例**
    - 2002年，Oracle CEO (拉里、艾里森)面對外面追問承認，Oracle一直雇用私家偵探去翻微軟技術協會的垃圾桶，試圖找到這個組織行賄以便影響反托拉斯案的審理證據。



47

技術性的社交工程方式

- **網頁或郵件的連結(Phishing)**
- **瀏覽網頁時彈出的視窗(Popup Windows)**
- **使用有趣的軟體(利用網頁/賭博遊戲的網站)**
- **垃圾郵件**
- **即時通訊的連結**

48

技術性的社交工程方式

- Phishing

  這類通常是以合法的商業組織為來源的電子郵件方式出現，這些組織通常是銀行、信用卡公司。郵件通常告知使用者必須再重新確認他們的個人資料，若不儘速回復可能會造成重大的損失。

  這些郵件通常會附上一個看似真正網站的連結、該公司的商標來獲取你的信任。讓你在上面輸入你的帳號、密碼、信用卡號碼甚至是你詳細的資訊。

技術性的社交工程方式

- Vishing (VoIP + Phishing)

  這是藉由VoIP的技術與金融部門的回復來騙取個人私密資料的和金融上的訊息。

  Vishing的攻擊方式結合了語音與網路釣魚的方式。藉由假造的網站與電話的服務去讓被害者去信任網站上公開的訊息，甚至去支付攻擊者所提供的帳單。

  習慣上使用者會認為這間金融公司是實際認知上的那家。實際上它是透過VoIP將它轉到網路上一個虛擬的公司，這是一個利用高明手段來進行詐騙。

Vishing

技術性的社交工程方式

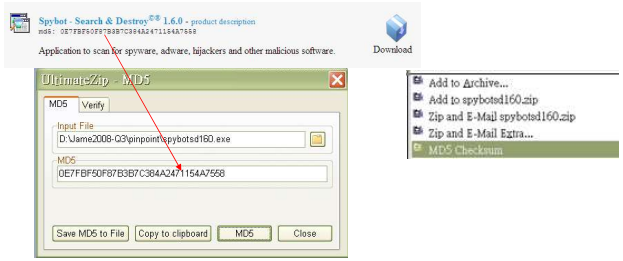
- 彈出的視窗Popup Windows

  攻擊者使用程式跳出一個欺騙的視窗，內容指出由於應用程式連線有問題，所以需要使用者重新輸入ID與Password來維持目前的連線。不會懷疑這件事的使用者會立即的去回應這件事情，因為他希望能夠繼續他的工作。即使在後來被告知，系統已被駭客破壞，還不知道是誰為駭客開了另外一扇門。

技術性的社交工程方式

- **有趣的軟體Interesting Software**

  受害者下載並安裝了自己有興趣的軟體，而這個軟體已被駭客加入木馬或病毒。



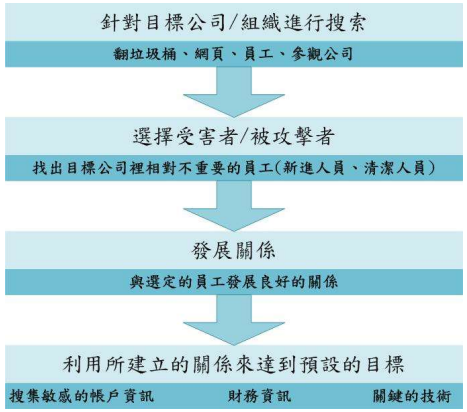
技術性的社交工程方式

- 垃圾郵件Spam Mails

  匿名者可以藉由電子郵件讓使用者在網際網路上植入惡意程式，它是將郵件寄給數百甚至數千的使用者。若使用者回復該信件便可能會成為特定的目標，進而造成更大的危害。

- **即時通訊的社交工程**

社交工程進行的步驟



社交工程的延伸

- 社交網路
  - **最早的網路社交的媒介多為文字模式進行，如MUD(Multi-User Dialogue，多人交談)、BBS(Bulletin Board System，電子佈告欄系統)**
  - **因為網路技術的提昇部落格(Blog)、微網誌(microblogging)也陸續的興起**
  - **近來更因為臉書(FaceBook)、撲(噗)浪(Plurk)、推特(Twitter)等社交網站的興盛，造成了所謂的社群網戰(Social Network)**

社交網路(資安)影片欣賞

世新大學廣電系-匿名遊戲

57

影片中您看到了什麼?

- 免洗ID?
- 劇情中看了表特版中的正妹照片後怎樣了？
- 女主角真的叫張榕容嗎?
- 張榕容上網的理由是甚麼？真正目的？
- 怎麼知道站務人員管理者帳號的?
- 管理者帳號的密碼有甚麼特色?
- 網路上的資料要如何填寫?
- 其他....

58

社交網路的威脅

- 社交網路已成為社交工程蒐集的目標
- 個人訊息與專業訊息的交叉混雜
- 社交網路的應用程式被利用
- 身份假冒與針對性的個人訊息攻擊
- 身份竊取
- 垃圾郵件與殭屍網路

59

社交網路的威脅(續)

- **社交網路已成為社交工程蒐集的目標**
  - 社交網路已為社交工程的攻擊者提供一個良好的資訊蒐集平台。
  - 攻擊者可利用目標的朋友清單，來了解目標的人際關係，並利用此關係讓目標加為好友，使用者大多分享在上面的資料都可以被獲取。
- **個人訊息與專業訊息的交叉混雜**
  - 即使您確定將社交網站的某個帳戶僅用於私人用途，另外一個帳號使用在某些專業的網站中，這也無法保證前者的圖片絕對不會出現在後者的帳號中，共同有的朋友不會將之間的關係不經意的讓老闆知道。

60

社交網路的威脅(續)

- 社交網路的應用程式被利用
  - 駭客利用社交網路上可自行編寫程式分享的功能，散播惡意程式或者入侵使用者帳號而在該使用者分享的程式中增加惡意程式。
- 身份假冒與針對性的個人訊息攻擊
  - 被惡意的人偽冒自己的身分(比如：將相片置於網路上，假藉名義進行惡意行為)。
  - 網路霸凌(揭露特定人士訊息)。
  - 社交網站的成員及時更新了自己的行為，也會導致許多”有心人“可以利用的狀況發生。比如：在上面敘述自己的旅行計畫，可能導致竊賊對您進行闖入/偷竊。

61

社交網路的威脅(續)

- 身份竊取
  - 簡單來說，身分竊取是指通過假裝一個人的身分而進行詐欺、竊取資料等來獲取非法的利益。使用者在社交網路的訊息通常都會透露出一些頗有價值的內容，想要進行身分竊取的人可以利用蒐集到的訊息，來猜測使用者的密碼或者假冒身分向管理人員取得授權，最後竊取其身分。

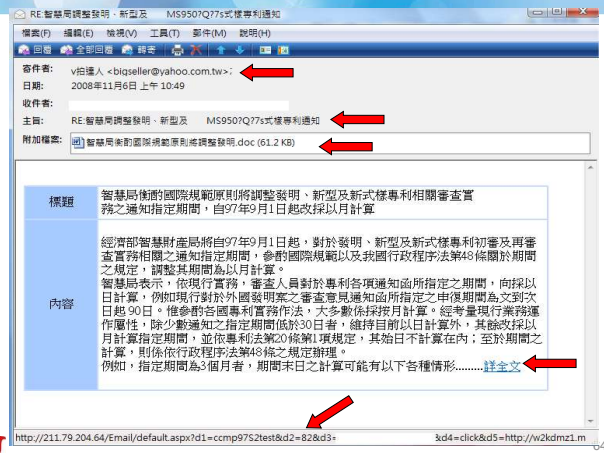
62

社交網路的威脅(續)

- 垃圾郵件與殭屍網路
  - 透過垃圾郵件傳遞訊息已經成為一項巨大的產業，廣告、網路釣魚、殭屍網路需要**有效的散播**、惡意軟體均是利用此途徑。攻擊者早已經滲透到社交網路中，劫持用戶帳號、使用其聯絡人清單傳播垃圾郵件、蠕蟲或其他惡意軟體。
  - 在國外著名的社交網站中已經發現，越來越多的惡意軟體都被當成附件放在垃圾郵件中。這類的郵件的特點是將不明真相的人吸引到”特殊的“網頁中，如引誘使用者點擊一個精彩的影像鏈結，而實際上是一個木馬的下載鏈結，偷偷將程式裝在使用者的電腦上，成為殭屍網路的成員。

63

釣魚郵件範例

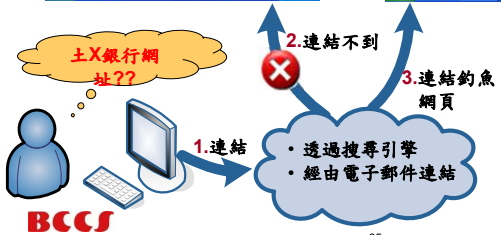


64

網頁釣魚風險

http://www.landbank.com.tw

http://www.1andbank.com.tw 釣魚網頁



例如：

遊戲X子

http://tw.gamania.com

vs. http://tw.gamannia.com

聯X銀行

http://www.ubot.com.tw

vs. http://www.obot.com.tw

65

網路釣魚(續)

66

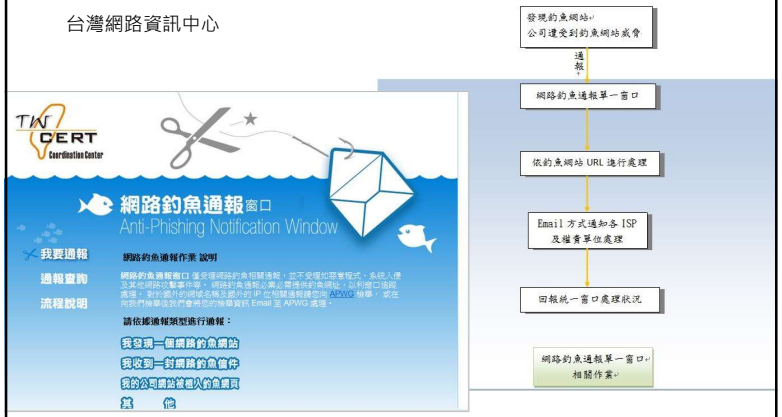
網路釣魚(續)

67

釣魚網站通報-台灣電腦網路危機處理暨協調中心

http://www.apnow.tw/index.cgi

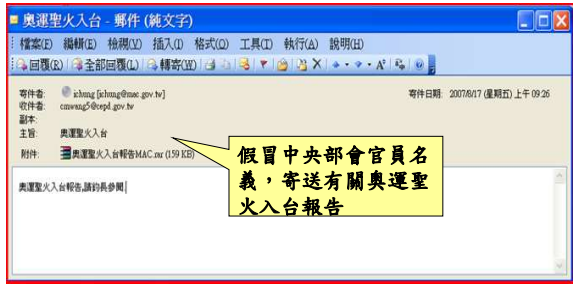
台灣網路資訊中心



68

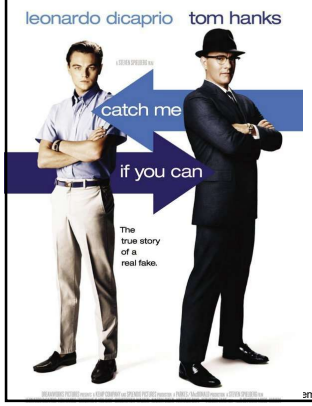
魚叉攻擊植入木馬程式案例

- 釣魚郵件不隨意發送，僅針對少數特定對象
  - 鑑識發現惡意連線軟體來自郵件，且收信人僅部會首長機要秘書一人
  - 進一步查證發現共有三個部會首長的機要秘書收到該釣魚郵件



影片欣賞

- 神鬼交鋒-利用汎美機師身分進行財務詐騙



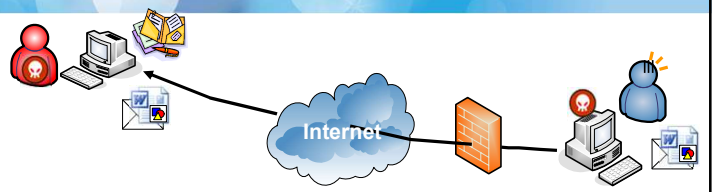
影片中您看到了什麼?

- 男主角假冒甚麼身分騙財?為什麼?
- 男主角為什麼挑選年輕的銀行窗口服務人員進行詐騙?
- 男主角在甚麼時候得知
  - 機師服裝來源
  - 兌換支票的最高金額
  - 機場櫃檯可以兌換支票
  - 支票號碼的意義
  - 可以搭乘順風機
  - ……
- 男主角的目的??????

電子郵件社交工程

BCCS 漢昕科技股份有限公司
Business Continuity Computing System Inc.

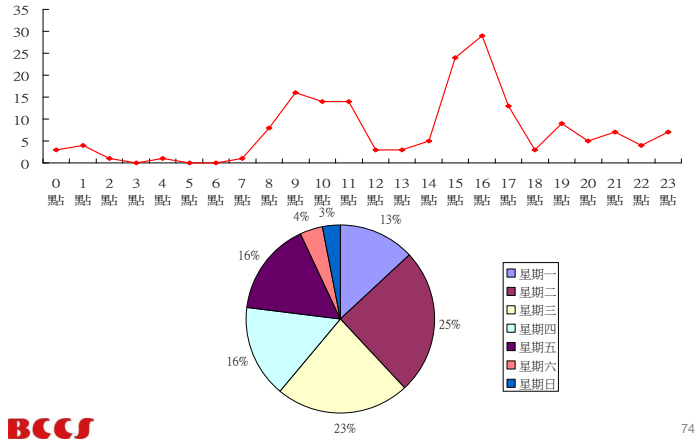
電子郵件社交工程攻擊模式



1. 駭客設計攻擊陷阱程式(如特殊*Word*檔案或外部惡意連結)
2. 將攻擊程式置入電子郵件中
3. 寄發電子郵件給特定的目標
4. 受害者開啟電子郵件
5. 啟動駭客設計的陷阱，將被植入後門程式
6. 後門程式逆向連接，向遠端駭客報到

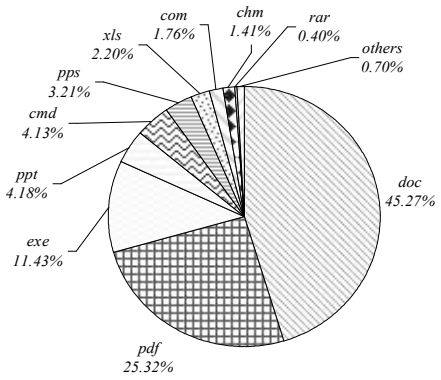
73

社交工程攻擊具針對性



74

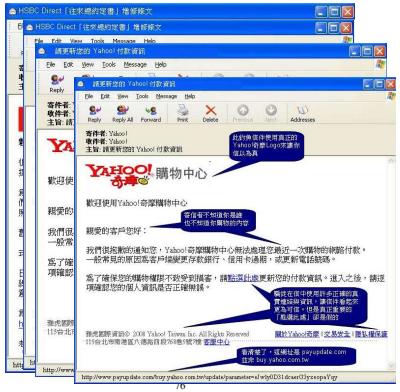
社交工程電子郵件附件檔案



75

判斷是否為社交工程電子郵件

- 以下的郵件是否為網路釣魚的電子郵件?



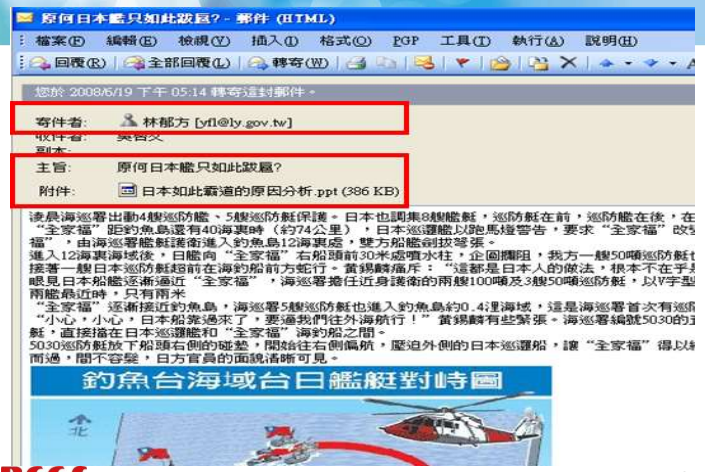
76

社交工程郵件案例

- 八卦影視
- 休閒娛樂
- 保健養生
- 財經資訊
- 情色內容
- 新奇資訊

77

惡意電子郵件範例

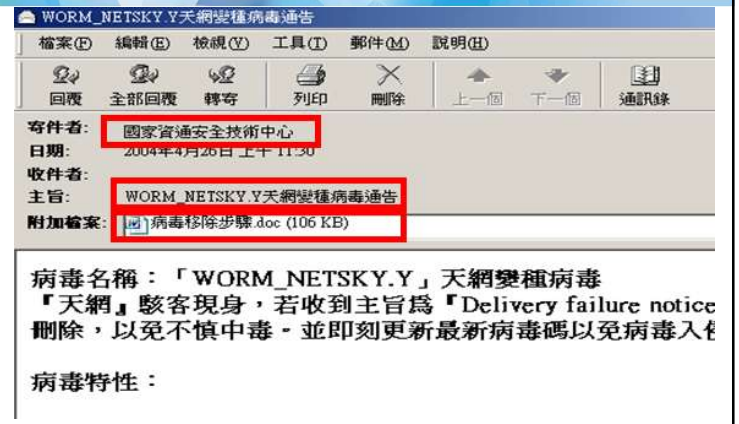


78

惡意電子郵件範例

79

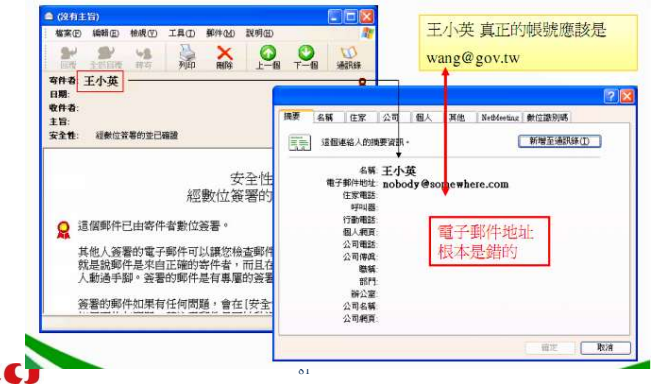
惡意電子郵件範例



80

惡意電子郵件範例

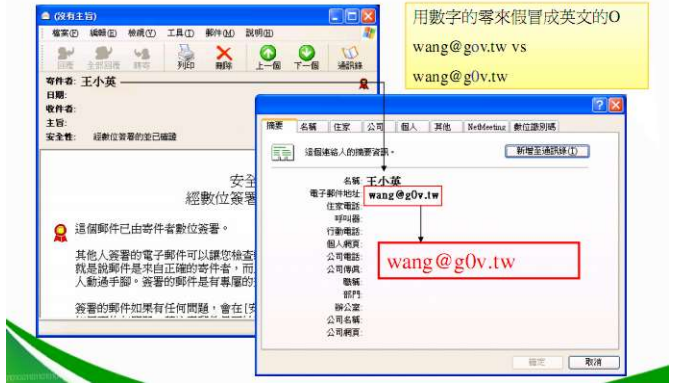
假冒寄件者方式－顯示名稱假冒



81

惡意電子郵件範例

假冒寄件者方式－電子郵件帳號假冒



82

社交工程攻擊之防範

- **建立社交工程**防範技術措施*(Engineering)*
- **辦理相關**宣導及法治認知*(Enforcement)*
- **加強**資安訓練與演練*(Education)*

83

83

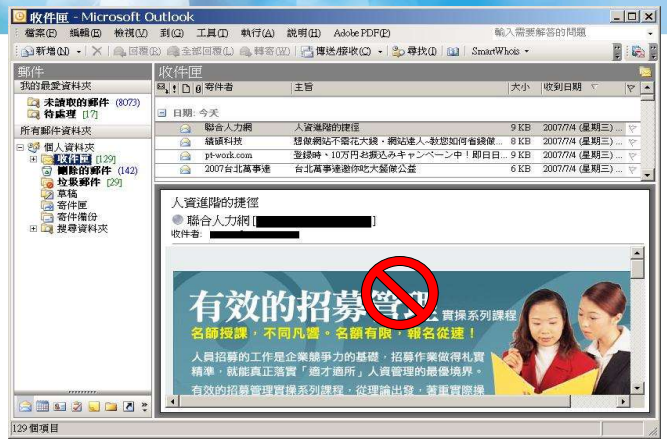
使用者防護停看聽(1)

- 停 ─ 使用任何電子郵件軟體前，必須先確認以下設定
  - 必須安裝防毒軟體，並確實更新病毒碼
  - 審慎開啟郵件及其附件或連結
  - 必須取消郵件預覽功能，避免無意開啟郵件
  - 設定過濾垃圾郵件機制
  - 建立電子郵件驗證機制(推動電子識別證)

84

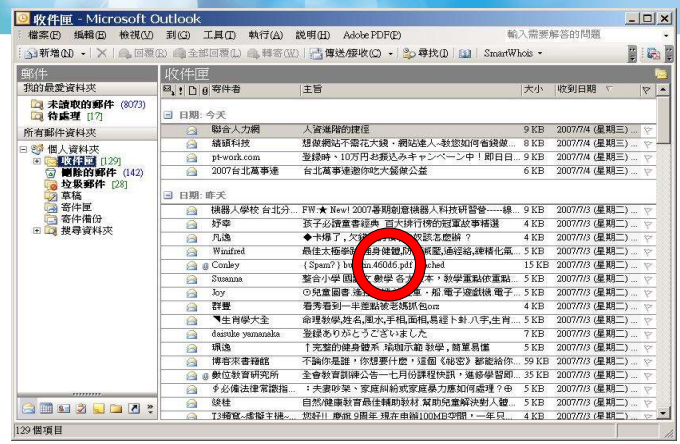
84

取消郵件預覽功能



85

取消郵件預覽功能(續)

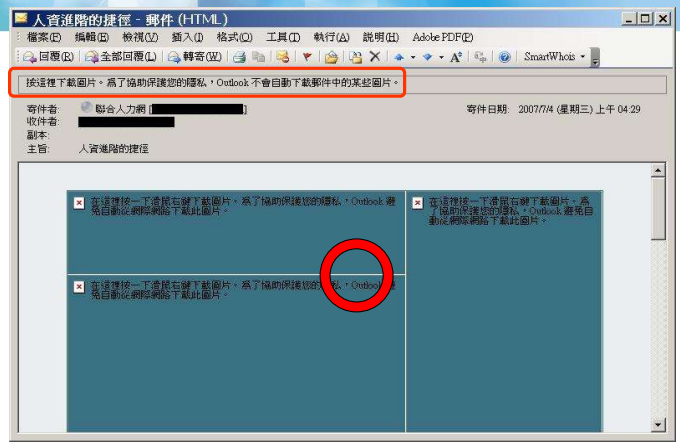


86

關閉郵件自動下載圖片及其他內容

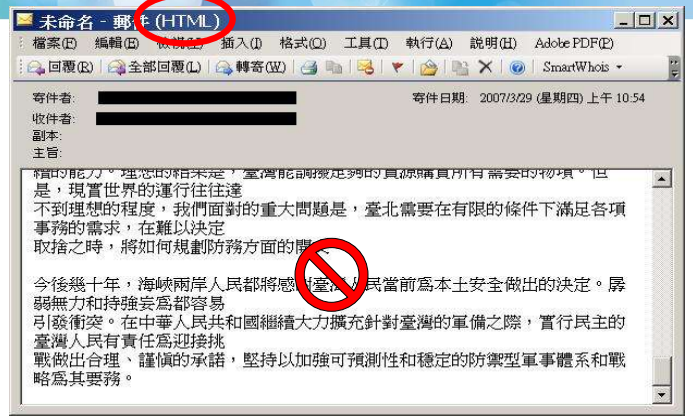
87

關閉郵件自動下載圖片及其他內容(續)



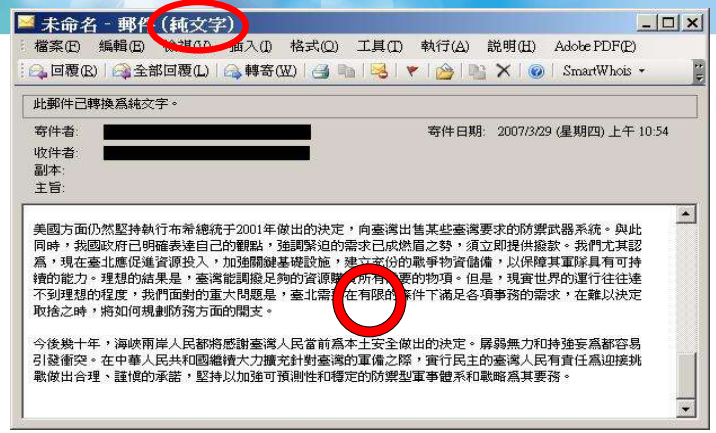
88

不以HTML模式開啟郵件



89

以純文字模式開啟郵件



90

使用者防護停看聽(2)

- 看 – 收到郵件後，必須注意
  - 郵件主旨是否與本身業務相關
  - 其餘郵件不建議開啟，如需開啟應確認郵件來源
- 開啟電子郵件前應先依序檢視：
  (1)【寄件者】
  (2)【郵件主旨】
  (3)【附加檔案】等郵件訊息
- 【寄件者】或【郵件主旨】與公務無關者，建議應立即刪除不要開啟郵件

91

使用者防護停看聽(3)

- 聽 – 若懷疑郵件來源，必須進行確認
  - 透過電話或電子郵件向寄件人於開啟前確認郵件真偽

92

使用者端郵件安全管理

93

93

日常作業的資訊安全

BCCS 漢昕科技股份有限公司
Business Continuity Computing System Inc.

94

資料夾分享

- 限制資料夾共享權限，避免不適當之權限設定，造成機敏性資料遭到未經授權存取。(例如：**讀取權限為Everyone**)

95

敏感級以上資料須確實上鎖

同仁下班時應確實將涉及機敏及個資之文件放置於可上鎖之抽屜並於離開時上鎖。

96

96

嚴禁手機使用個人電腦USB充電

97

97

windows update 及防毒更新

- 同仁需確認定期(週、月) 將設備開機並完成更新作業。
- 確認單位行動設備(筆電)或較少使用之資訊設備各項更新作業
  - windows update
  - 防毒軟體、病毒碼更新

98

98

windows update 及防毒更新 (續)

Help me!!

同仁於日常作業中如有任何電腦上的異常，如**windows**更新失敗、防毒軟體發現惡意軟體(病毒)等，均需與資訊室做通報。

99

99

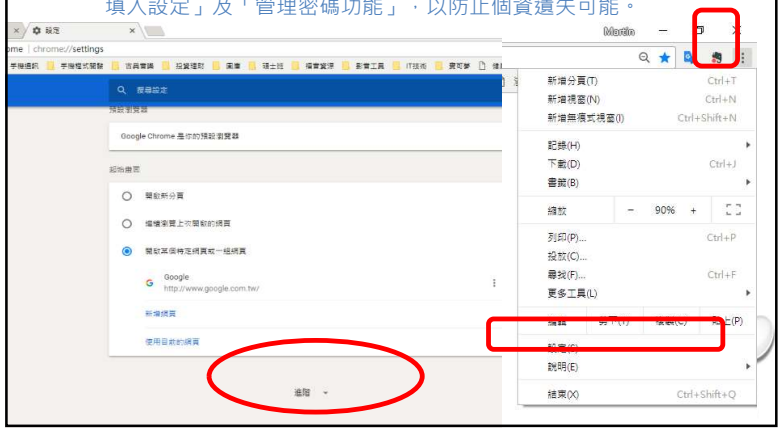
定期清空資源回收桶或直接刪除

100

100

別讓瀏覽器自動幫你紀錄及填寫密碼

- 同仁使用google chrome瀏覽器，應關閉「密碼和表單」的「自動填入設定」及「管理密碼功能」，以防止個資遺失可能。



101

別讓瀏覽器自動幫你紀錄及填寫密碼(續)

102

日常作業中使用電腦注意事項(1)

- **密碼的管理**
  - 不告訴任何人密碼（包括親人、職務代理人、上司等）。
  - 不寫下密碼。
  - 設定不容易被猜到的密碼。
  - 一旦懷疑有人知道您的密碼，即刻更改。
- **軟體更新**
  - 隨時留意作業系統更新功能與提醒。
  - 不使用盜版軟體。
- **病毒的預防**
  - 防止電腦病毒的第一法則:安裝防毒軟體，並且定期更新病毒碼。

103

日常作業中使用電腦注意事項(2)

- **安全的電腦操作環境**
  - 電腦操作環境應保持乾燥清潔、避免飲食。
- **資料備份**
  - 將重要檔案複製到電腦硬碟以外的儲存硬體，例如：光碟片、網路硬碟等。
  - 定期測試備份資料是否有效。
- **Cookie記錄**
  - 透過設定瀏覽器的安全設定值來限制Cookie功能，路徑為瀏覽器的「工具」->「網際網路選項」->「隱私權設定」。

104

日常作業中使用電腦注意事項(3)

- **隱私權**
  - 在網路上留下個人資料前，先閱讀該網站的「隱私權保護政策」內容 。
  - 不要任意在從來沒有聽過或第一次造訪的網站中填寫重要的個人資料或留下信用卡資料。
- **公用存取**
  - 特別留意坐或站在旁邊的人。
  - 不勾選瀏覽器的「記住密碼」選項。
  - 離開前應完成「登出帳號」動作後，再關閉瀏覽器。
  - 盡量不在公共電腦中輸入敏感性高的資料。

105

日常作業中使用電腦注意事項(4)

- **垃圾電子郵件**
  - 絕不回覆垃圾電子郵件。
  - 不回應、購買垃圾電子郵件的廣告商品。
- **間諜軟體**
  - 下載免費或共享軟體前，需仔細閱讀和軟體有關的所有訊息。
  - 避免透過P2P程式或其他管道下載來路不明軟體。
- **網路毀謗**
  - 在網路上發言前，三思而後發布。
  - 不隨意轉寄未經證實的網路流言信件等。

106

日常作業中使用電腦注意事項(5)

即通訊軟體

--不隨意接受透過即時通所傳遞來的檔案。

--不透過即時通傳遞個人資料，或重要的機關機密資料。

智慧財產權

--避免觸犯其他網站的商標或著作權

網路釣魚與網路詐騙

--不直接使用email所提供的超連結，以自己輸入網址方式取代

--凡事求證後才行動，可減少被騙機會。

107

謹慎使用公務用電子信箱

- 公用電子信箱應僅公務使用，非公務之外部服務應使用個人信箱(yahoo,google等)。

108

電子郵件社交工程的特徵

- 過於聳動的主旨與緊急要求。
- 不正常的發信時間。
- 陌生人或少往來對象來信。
- 認識的人來信但主旨或內容與其習性不符。
- 要求輸入私密資料送出。
- .....

109

電子郵件社交工程的防範機制

- 關閉使用者客戶端收信軟體的郵件預覽功能
- 使用純文字模式來讀取電子郵件
- 不開啟來路不明或與本身業務不相關之電子郵件
- 不點擊電子郵件內的不明網路連結
- 打開附件前先用防毒軟體進行掃描
- 避免在網路上公開自己的電子郵件帳號
- 定期更新 Windows 與 office 修補程式，且更新瀏覽器版本，避免因系 統軟體 bag 造成安全漏洞
- 定期更換密碼

110

Thank you

111