111年第1梯次資通安全通識教育訓練

資深顧問師 彭至賢 (Sam Peng)

ISO27001/BS10012/ISO9001主導稽核員

PMP/MCSE/CCNA/TPIPAS管理師&驗證師

TTQS人才發展品質管理系統-評核委員

Mobile: 0952-695460

E-mail: sam@safelink.com.tw

SafeLink 博創資訊科技股份有限公司

課程大綱(Agenda)

- 本校資安宣導及推廣事項
- 從案例中探討資訊安全(含隱私權衝擊)
- 新冠肺炎疫情衝擊下資訊安全威脅(含資訊科技新知)
- 社交工程與案例分析(含勒索病毒+釣魚郵件)

禁用大陸資通訊產品宣導

- 行政院重申各公務機關使用資通訊產品（含軟體、硬體及服務）相關原則：
- (一)公務用之資通訊產品不得使用大陸廠牌，且不得安裝非公務用軟體。
- (二)個人資通訊設備不得處理公務事務，亦不得與公務環境介接。
- (三)各機關應就已使用或採購之大陸廠牌資通訊產品列冊管理，且不得與公務環境介接。

本校資通安全政策宣導

- 一、本校各項資訊安全管理規定必須遵守政府相關法規（如：資通安全管理法及相關子法、刑法、國家機密保護法、專利法、商標法、著作權法、個人資料保護法等）之規定。
- 二、 實施資訊安全教育訓練，宣導資訊安全政策及相關實施規定。
- 三、 建立資訊硬體設施及軟體之管理機制，以統籌分配、有效運用資源。
- 四、 新資訊系統應於建置前將資訊安全因素納入，防範危害系統安全之情況發生。

本校資通安全政策宣導

- 五、 建立機房實體及環境安全防護措施，並定期施以相關保養。
- 六、 明確規範資訊系統及網路服務之使用權限，防止未經授權之存取行為。
- 七、 訂定資訊安全之營運持續計畫並實際演練，確保本校資訊業務持續運作。
- 八、 資訊安全政策應定期進行評估，以反映資訊安全管理、法令、技術及本校業務之最新狀況，並確保本校資訊安全實務作業之可行性及有效性。

SafeLink – We Secure Your Network and Content.

本校資通安全目標宣導

- (一) 年度目標之評量機制之各項記錄應彙整成「資訊安全目標管理查核表」，以便追蹤當年度內的達成績效。「資訊安全目標管理查核表」應包含下列事項：1.待辦事項2.所需資源3.負責人員4.完成時間
- (二) 若報表之記錄/趨勢顯示相關之事件發生次數，即將可能達到或超過年度目標之設定值，則必須依照「改善作業管理說明書」之規定填寫「矯正措施/持續改善表」，以便於失效前提出矯正措施。

資安及個資保護專區宣導

- 本校資安及個資保護專區網址：
  https://cc.ntcu.edu.tw/

SafeLink – We Secure Your Network and Content.

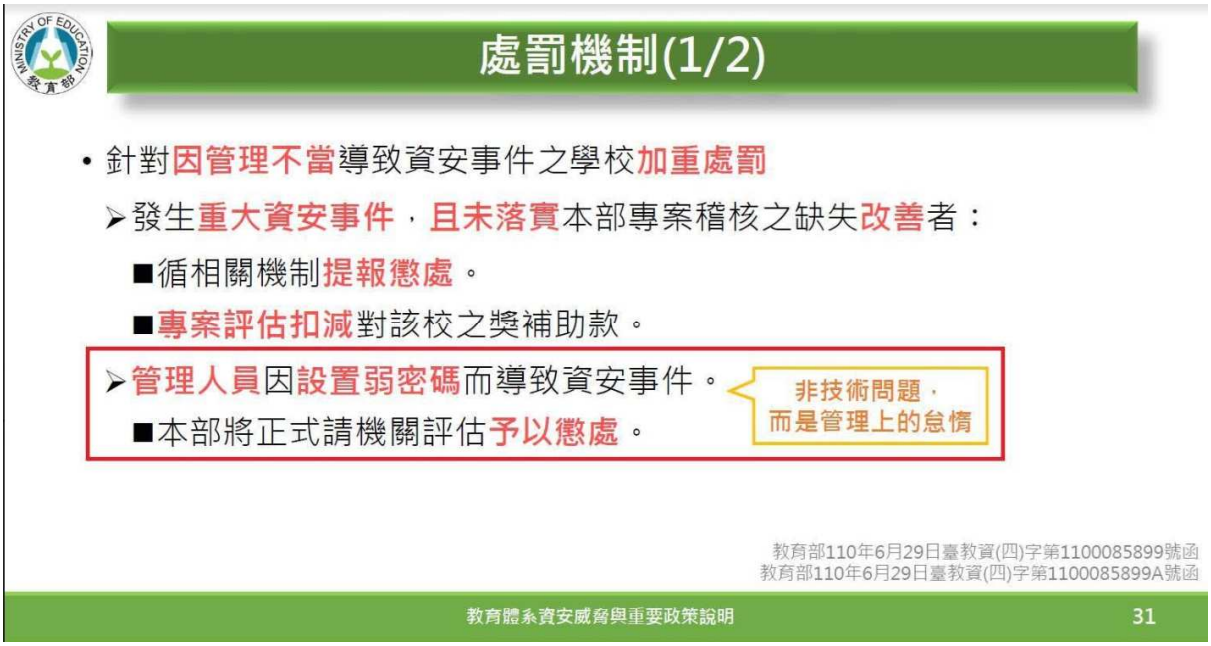
校園保護智慧財產權行動方案

- 教育部來函 執行110學年度大專校院「校園保護智慧財產權行動方案」自評表及填表說明，依自評表檢核指標落實執行
- 110學年度大專校院執行「校園保護智慧財產權行動方案」自評表：

(十五)對於疑似侵害智慧財產權之主機，應視不同之程度與狀況採取必要作為，並進行相關宣導措施及留下有關之處理與宣導紀錄。	學校是否對於疑似侵權之主機，採取相關處理措施，並進行宣導及紀錄之？	☑是 ☐否	請說明處理疑似侵權主機之情形： (1).處理措施流程及方式：列入資安管制清冊，並以正式公文通知使用單位處理。 (2)宣導內容：(請提供相關內容) 請尊重智慧財產權，勿使用 p2p 軟體下載非法軟體或影音資料以免觸法。 (3)本學年共 0 件 (4)承上題，如有發生，請簡述處理情形：

SafeLink 博創資訊

教育體系資安威脅與重要政策說明



業管相關系統/網站/設備密碼設定原則

- 應檢核不得使用弱密碼、預設密碼，並符合規範之密碼複雜度要求，以及依業務需求設定適當網路存取限制，請確認系統(網站)設定密碼原則已符合行政院規定：
- 1.通行密碼長度應至少八碼(系統管理者應至少十二碼)。
- 2.使用者每九十天應更換通行密碼，密碼最短使用期限應至少一天。
- 3. 通行密碼應避免重複使用前三次變更之通行密碼。
- 4.禁止使用者共用帳號及通行密碼。
- 5.禁止使用身分證字號、學校代碼、易猜測之弱密碼或其他公開資訊等作為帳號及密碼。

業管相關系統/網站/設備密碼設定原則

- 應檢核不得使用弱密碼、預設密碼，並符合規範之密碼複雜度要求，以及依業務需求設定適當網路存取限制，請確認系統(網站)設定密碼原則已符合行政院規定：
- 6.不包含使用者的帳戶名稱全名中，超過兩個以上的連續字元。
- 7.密碼應包含下列四種字元中的三種：
- (1) 英文大寫字元(A 到 Z)。
- (2) 英文小寫字元(a 到 z)。
- (3) 10 進位數字(0 到 9) 。
- (4) 非英文字母字元(例如：!、$、#、%)。

教育部稽核前各請單位配合事項

- 所有自行或委外設置、開發、維運之系統承辦人皆應到場(K401)，委外廠商則建議提醒待命，若被抽查到，需要了解系統技術內容，再致電請廠商協助。
- 所有系統承辦人攜帶下列文件到場:
- 1. 系統契約書
- 2. 資訊系統安全等級評估表
- 3. 依安全等級評估表評定等級，所填寫資通系統防護基準檢核表

表單圖示如下：

系統安全等級評估表

「（系統名稱）」資通系統安全等級評估表

紀錄編號：YYYMMDD			填表日期：　年　月　日
功能說明：			

影響構面				資通系統安全等級
1. 機密性	2. 完整性	3. 可用性	4. 法律遵循性	

設定影響構面等級

影響構面	安全等級		原因說明
1. 機密性	初估		
	異動		
2. 完整性	初估		
	異動		
3. 可用性	初估		
	異動		
4. 法律遵循性	初估		
	異動		
備註			
承辦單位		資訊單位	

SafeLink – We Secure Your Network and Content.

資通系統防護基準檢核表

構面	類別	項次編號（原始）	最低系統等級要求	安全控制措施	是否符合	現況說明	佐證	矯正作為	目標日期	備註說明
存取控制	帳號管理	1	普	建立帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。	符合	依「ISMS_WI_016網站管理辦法」之規範，網站管理帳號變更/新增之申請，需填寫「流程服務管理系統」之「系統帳號/權限異動申請表」，由網站管理者進行變更/新增作業。	1. 系統帳號/權限異動申請表」 2. 帳號權限審核紀錄			
	遠端存取	10	普	對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化。	符合	本系統僅限以內部網路特定 IP 白名單連線至系統管理後臺，並禁止使用 VPN 連線。	1. 系統管理維護手冊 2. 系統本機防火牆設定			
		11	普	使用者之權限檢查作業應於伺服器端完成。	符合	於伺服器端實作 RBAC 集中授權機制。	系統功能規格書			

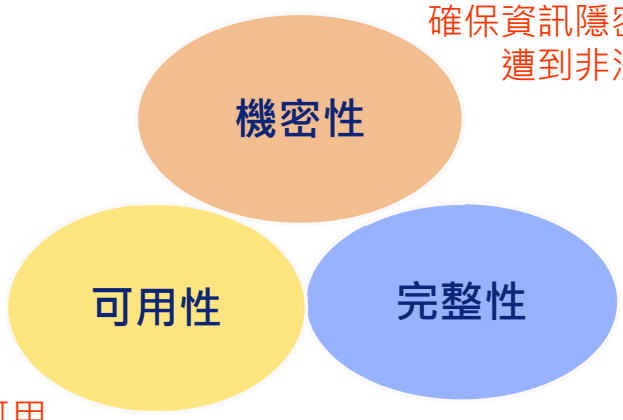
SafeLink 博創資訊

課程大綱(Agenda)

- 本校資安宣導及推廣事項
- 從案例中探討資訊安全(含隱私權衝擊)
- 新冠肺炎疫情衝擊下資訊安全威脅(含資訊科技新知)
- 社交工程與案例分析(含勒索病毒+釣魚郵件)

資訊安全釋義

- 資訊安全防護對象：資料
- 資訊安全的目標：資料的機密性、完整性、可用性



確保資訊隱密性並避免遭到非法存取

確保可適時提供可用及正確之資訊

確保可提供正確與完整的資訊

喪失機密性案例

- 瞞了一年，還付了 10 萬美金贖金!Uber 5700萬乘客與駕駛個資遭駭。
- Yahoo 認了，不只 10 億! 2013 年 30 億用戶帳號無一倖免，全數被駭。
- 臉書爆發個資外洩醜聞，已知8700萬用戶資料遭流出、20億用戶的權益恐受損。
- 臉書程式漏洞被駭客入侵，高達5000萬筆個資受影響，包括臉書創辦人兼執行長祖克柏及臉書營運長桑伯格的帳號在內。

SafeLink – We Secure Your Network and Content.

喪失機密性案例

網路詐欺案件層出不窮，主要在於個人資料外洩嚴重。**電視購物、網路購物、網路書店、 旅行社等業者頻頻出包**，讓詐騙受害人激增，一度讓政府束手無策，民眾惟有自覺性的提高警覺心，冷靜判斷、理性處理花招百出的詐騙手法。

喪失機密性案例

喪失完整性案例

- 飛美頭等艙50萬賣3萬！ 國泰航空霸氣認賠
- 聯合新聞網 2019-01-03
- 國泰航空官網訂票系統疑因出錯，乘客訂購越南或美國出發航班的商務艙，來回原價折合新台幣近五十萬元機票只要兩萬多元，約為原價百分之五。國泰昨在臉書粉絲團認賠，宣布「限時頭等艙與商務艙機票快閃」，等於「霸氣」全數承認便宜機票。

- 文末還自我解嘲「新一年繼續多多指教」、「從小就學會錯就要認」，國泰的回應與處置，贏來網友大讚「欣賞負責的態度」。

喪失完整性案例

- 國泰航空系統又出包！49萬頭等艙「票價少個0」
- 東森新聞 2019-01-14
- 國泰航空售票系統又出錯！繼日前標錯頭等艙價格後，香港國泰航空昨（13）日又被網友發現有歐洲航線的頭等艙機票，以原價約1折販售，原價1.6萬美元（約新台幣49萬元）的機票只要1512美元（約新台幣4.6萬元）就能買到。
-
- 對此，國泰已承認票價輸入錯誤，仍大方表示「對極少數買到這些機票的客戶，我們期待迎接您登機，來享受我們的優質服務。」

喪失可用性案例

- 全台郵局ATM、儲匯窗口當機 Yahoo奇摩 2019年7月24日

中華郵政電腦系統全台大當機，中華郵政表示，影響範圍為儲匯窗口跟ATM，當機原因不明，上午10時25分系統陸續恢復正常，但發生原因仍待查。
中華郵政今天早上8時35分時系統當機，導致儲匯窗口跟ATM無法使用，上午10時25分陸續修復，發生原因仍待查。

Q1：請問這是喪失哪種資料保護特性？

- **開山里簡訊擾人 疫情警示出包**
- 中國時報 2019-07-10
- 7/9日中午很多人的手機螢幕出現「開山里登革熱疫情注意」的細胞簡訊，這是今年衛福部疾管署首次發出登革熱疫情的訊息，事後發現是「細胞廣播系統出現bug」，導致全國民眾收到簡訊，造成困擾。

因資安問題升級到2016年版，過程中程式搬遷出問題而把開山里周邊390公尺變成公里，這是疾管署的系統出錯，疾管署特向國人道歉

情資分享：個資外洩案例分享(一)

情資分享：個資外洩案例分享(一)

發生時間	2020/05/30
事件概述	美國資安公司 Cyble Inc 29日報告指出，發現台灣超過2000萬人的戶政資料被登上暗網販售，標題為「台灣全國戶政登記資料庫（Taiwan Whole Country Home Registry DB）」；根據**該賣家所稱，這些資料是2019年從台灣內政部戶政司竊取而來**。 調查局資安工作站30日接獲消息後隨即啟動偵辦，這些資料共有3.5GB、超過2000萬筆，**內容包括姓名、生日、地址、電話等個資**，資安站根據格式研判，外流的個資建檔時間從2001年到2008年間不等，距今10幾年，屬於舊資料，使用價值不高。 而從內容來看，資料欄位跟現在的格式不同，**無法斷定一定就是從政府單位外流，且有拼貼的跡象，亦可能是多個民間企業主機竊取而來**。

SafeLink – We Secure Your Network and Content.

情資分享：個資外洩案例分享(一)

問題分析	**若為政府機關流出，則應檢視戶政單位之資安/個資管理系統運作之狀況；若為政府機關委外單位(即民間企業)流出，則須檢視政府機關是否做到「個人資料保護法施行細則第8條」之相關委外監督之管理。**
防範方式	1. 公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。 A. 配置管理之人員及相當資源。 B. 界定個人資料之範圍。 C. 個人資料之風險評估及管理機制。 D. 事故之預防、通報及應變機制。 E. 個人資料蒐集、處理及利用之內部管理程序。 F. 資料安全管理及人員管理。 G. 認知宣導及教育訓練。 H. 設備安全管理。

情資分享：個資外洩案例分享(一)

防範方式	I. 資料安全稽核機制。 J. 使用紀錄、軌跡資料及證據保存。 K. 個人資料安全維護之整體持續改善。 2. 委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適當之監督。
衝擊影響&省思	1. 個資外洩事件的頻傳，儼然以對民眾隱私權衝擊造成甚大影響，進而造成詐騙事件屢屢增加，這些皆是政府機關、民間企業仍須努力改進的地方。 2. 該案件之個資外洩範圍被政府機關認為"使用價值不高"，但**即便是使用價值不高亦須謹慎追究資料流出之方式，進而採取相關防護措施**。

情資分享：個資外洩案例分享(二)

情資分享：個資外洩案例分享(二)

發生時間	2020/05/13
事件概述	新冠肺炎疫情趨緩，新北市運動中心才解封不到10天，就被爆出實名制資料外洩情形，網友在ptt發文表示，**新北市運動中心保存的個資，不但可以在網路上公開瀏覽，甚至還能刪除、修改內容，完全沒設任何權限**，讓網友看傻眼，甚至還有人惡搞，在表單上貼罷韓文宣，對此新北市體育處回應，初步調查是**被駭客入侵**。
問題分析	此運動中心因使用Google表單蒐集個資，對蒐集之個資檢視修改等權限未適當把控，引起駭客惡意入侵。
防範方式	1. 不使用網路共享雲端蒐集/處理/利用太過敏感之個資檔案。 2. 若使用雲端傳輸檔案，應對檔案進行適當**加密**，以免個資外流。
資料來源	https://www.youtube.com/watch?v=BBBb9qa8oLA

情資分享：個資外洩案例分享(三)

情資分享：個資外洩案例分享(三)

發生時間	2020/08/16
事件概述	刑事局表示，網路書店「TAAZE讀冊生活」疑會員個資外洩，統計顯示今年1月至8月9日達230人受騙，財損逾新台幣2200萬元。 刑事局指出，**消費者於「TAAZE讀冊生活」購書後，隨後接到佯裝客服人員的詐騙電話因而受騙。**刑事局解釋，這類詐騙手法是老招再更新，呼籲民眾接到類似電話要小心謹慎。 張天立接受中央社記者訪問表示，「TAAZE讀冊生活」長期致力加強網路資安防護，今年再升級防護網，本月網站遭受攻擊也即時掌握。

SafeLink – We Secure Your Network and Content.

情資分享：個資外洩案例分享(三)

問題分析	「TAAZE讀冊生活」長期以來網站遭到攻擊、竊取個資的問題，表示現行的資安防護機制稍顯薄弱。 目前資訊攻擊手法日新月異，若沒有即時更新相關資訊與新知，便容易出現資安漏洞。
防範方式	依個人資料保護法第 27 條規定： 非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。 前項措施，得包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則： 一、配置管理之人員及相當資源。 二、界定個人資料之範圍。 三、個人資料之風險評估及管理機制。

SafeLink 博創資訊

情資分享：個資外洩案例分享(三)

防範方式	四、事故之預防、通報及應變機制。 五、個人資料蒐集、處理及利用之內部管理程序。 六、資料安全管理及人員管理。 七、認知宣導及教育訓練。 八、設備安全管理。 九、資料安全稽核機制。 十、使用紀錄、軌跡資料及證據保存。 十一、個人資料安全維護之整體持續改善。
衝擊影響&省思	1. **社群網站、網路商城(含購物平臺)、旅遊業者、網路書局及電視購物皆為個資外洩事件頻傳之產業**，民眾應提高警覺性，避免遭受詐騙集團詐騙得逞。 2. 詐騙集團最常使用的詐騙手法，即透過黑色產業鏈取得民眾個資後，**以ATM解除分期付款方式詐騙**。

SafeLink – We Secure Your Network and Content.

情資分享：個資外洩案例分享(四)

發生時間	2020/10/15
事件概述	國立ＯＯ大學通識教育中心於12日**向校內220位學生寄出講座通知信，當中竟夾帶104至108學年度全數新生共計8495筆個人資料**。學生質疑校方未妥善管理個資，且目前已有當事人準備提告。校方則於19日召開校務會議，說明事件始末，並提出加強教育訓練、成立個資保護及處理小組等補救方案。 此次遭外洩的個資包含學生姓名、身分證字號、電子郵件、行動電話等項目。事發隔日，通識中心緊急處理，**先後寄兩封信通知收到個資的220位學生，要求其協助刪除**。14日，中正資訊處**將此事通報至教育機構資安通報平台**，校方再依《個人資料保護法》第十二條規範，**以信件及簡訊通知個資遭外洩之當事人**。

SafeLink 博創資訊

情資分享：個資外洩案例分享(四)

問題分析	此事件承辦人為9月到職之新進同仁選錯夾帶檔案，雖校方出面說明乃是無心之過，但也顯示出相關承辦業務人員於個資教育保護觀念的不足。
防範方式	1. 存放於電腦中的某些高敏感個資（個資法第六條提到之病歷、醫療、基因、性生活、健康檢查及犯罪前科）建議於保存時即刻加密。 2. 含有個人資料的檔案以電子方式傳輸時，建議宜進行加密。 3. 新進同仁應充分接受相關個人資料保護教育訓練。
資料來源	https://news.cts.com.tw/unews/campus/202010/202010152018066.html https://www.youtube.com/watch?v=WrCyqucSwx8

SafeLink – We Secure Your Network and Content.

情資分享：個資外洩案例分享(四)

相關法條補充	個資法第 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。 個資法第 18條： 公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。 個資法第 28 條 公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。 被害人雖非財產上之損害，亦得請求賠償相當之金額；其名譽被侵害者，並得請求為回復名譽之適當處分。

SafeLink 博創資訊

情資分享：個資外洩案例分享(四)

相關法條補充	依前二項情形，如被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，**以每人每一事件新臺幣五百元以上二萬元以下計算**。 對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害賠償者，其合計最高總額以新臺幣二億元為限。但因該原因事實所涉利益超過新臺幣二億元者，以該所涉利益為限。 同一原因事實造成之損害總額逾前項金額時，被害人所受賠償金額，不受第三項所定每人每一事件最低賠償金額新臺幣五百元之限制。 第二項請求權，不得讓與或繼承。但以金額賠償之請求權已依契約承諾或已起訴者，不在此限。

七個造成資料外洩的原因

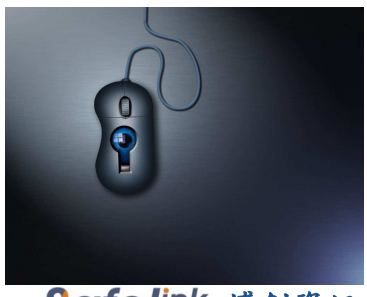
1.網路釣魚攻擊

以釣魚郵件將使用者引導至偽裝成真實購物網站、銀行、信用卡公司或網路服務等之合法登入頁面的假網站（釣魚網站），藉以竊取使用者在該網站所輸入的個資。

從你購物的網站偷偷**收集信用卡資訊**。因為新冠狀病毒(COVID-19,俗稱武漢肺炎)封城期間有更多使用者湧向電子商務網站，使得網頁卡號側錄相關的事件在三月增加了26%

2.盜用帳號:

Apple ID或Google、Amazon帳號等可連動多數網站服務的帳號在遭到盜用時，其受害情況很可能會擴及其他的網路服務。並且，帳號中所登記的信用卡資訊或姓名、住址等個人資料、雲端上的郵件或備份資料等私密資訊都可能會被盜取



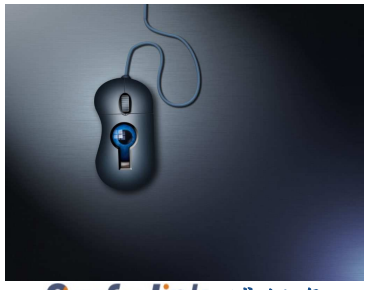
七個造成資料外洩的原因

3.惡意軟體或惡意應用程式的未授權操作

透過電腦或智慧型手機之未授權操作，可能會導致儲存資訊或輸入內容被監視，或裝置上的相機及麥克風等功能被用來竊取資訊。因此，不只是電腦，在智慧型手機上也需要安全防護對策

4.終端裝置遭竊或遺失

在電腦或智慧型手機中經常儲存了大量的資訊，例如聯絡方式、照片或影片、文件檔案、網站瀏覽器中儲存的各種網路服務的帳號與密碼，以及社群網站上的動態等。萬一終端裝置因遭竊或遺失落入惡意的第三方手中，可能會發生未授權操作而導致這些個資發生外洩。



SafeLink – We Secure Your Network and Content.

七個造成資料外洩的原因

5.在社群網站上過度公開資訊

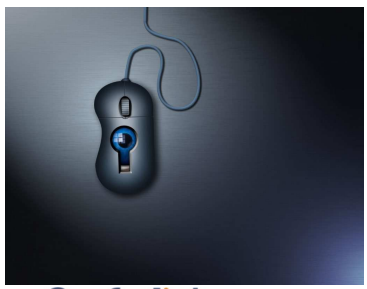
當使用Facebook、Instagram、Twitter或LINE等社群網站時，您可能會誤以為只有在朋友間分享，而導致過度公開個人資料。但是，您在網路上公開的個資可能被不特定多數的外人瀏覽。您不知道是什麼人以何種目的在瀏覽您的資料。這些人之中也存在專門收集資訊的第三方，會將資料用於犯罪用途，或賣給惡質的個資名單業者。

6.公共Wi-Fi 分享無線網路

分享無線網路使用上雖然很方便，如果沒有採取適當的安全防護對策，很容易就會發生通訊內容被監視的風險。駭客創造與公共Wi-Fi相似名稱的假熱點，讓您在不知情下登入以竊取個資的犯罪手法。

7.服務業者的過失或網路攻擊

使用網路上的服務一定會伴隨個資外洩風險。截至目前為止發生的使用者相關資料外流事件，都是因為服務業者在安全防護上的過失或內部犯罪，還有網路攻擊的非法存取等原因所導致。

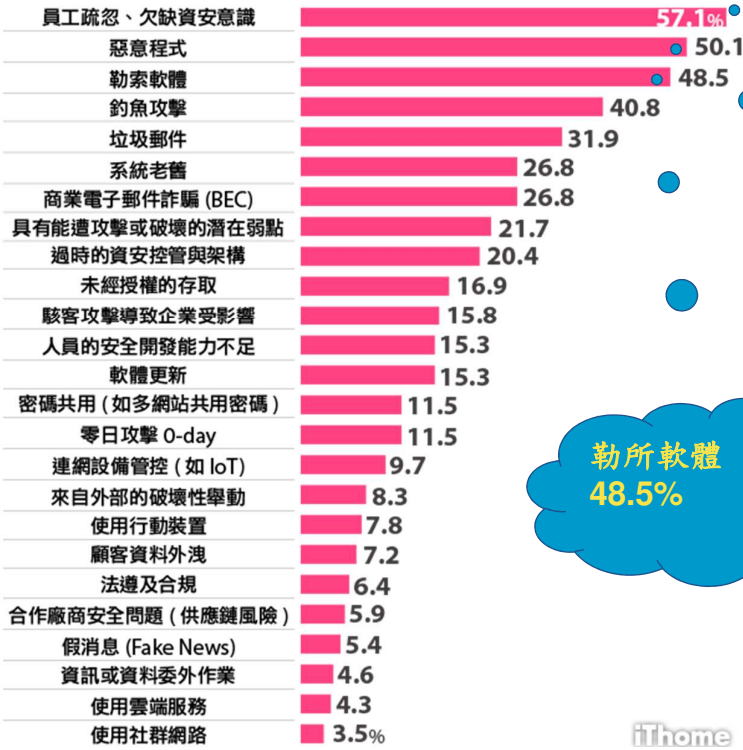


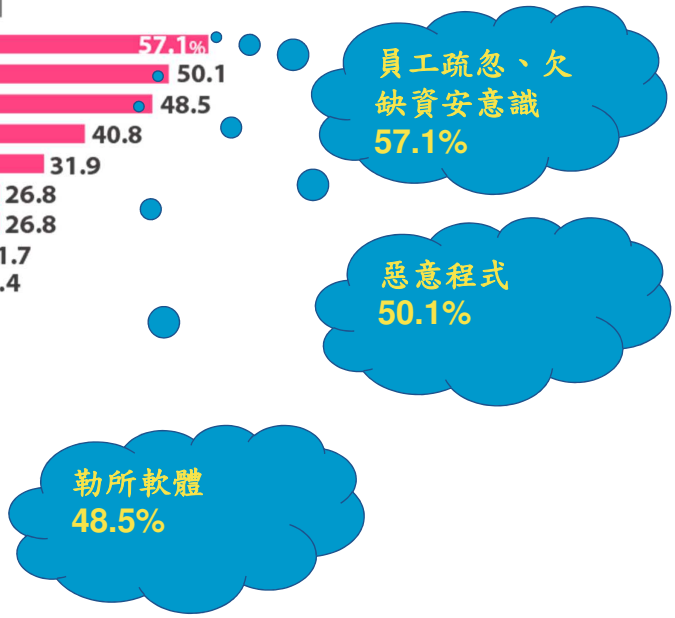
SafeLink 博創資訊

員工資安意識不足的威脅，比駭客更大

2020 企業資安風險 Top25

BEC 威脅大增，假新聞資安風險開始浮現



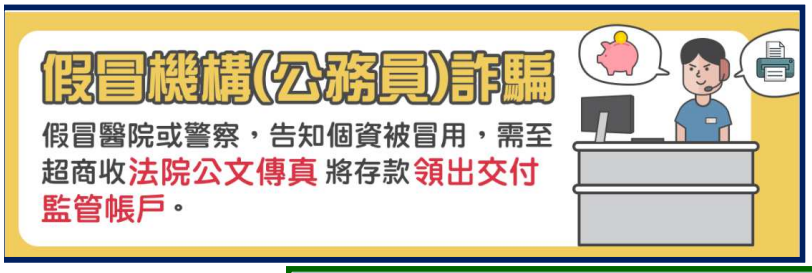


iThome

SafeLink 博創資訊

當你個資外洩時會發生什麼事？

詐騙集團可能會拿你的個資做的事情

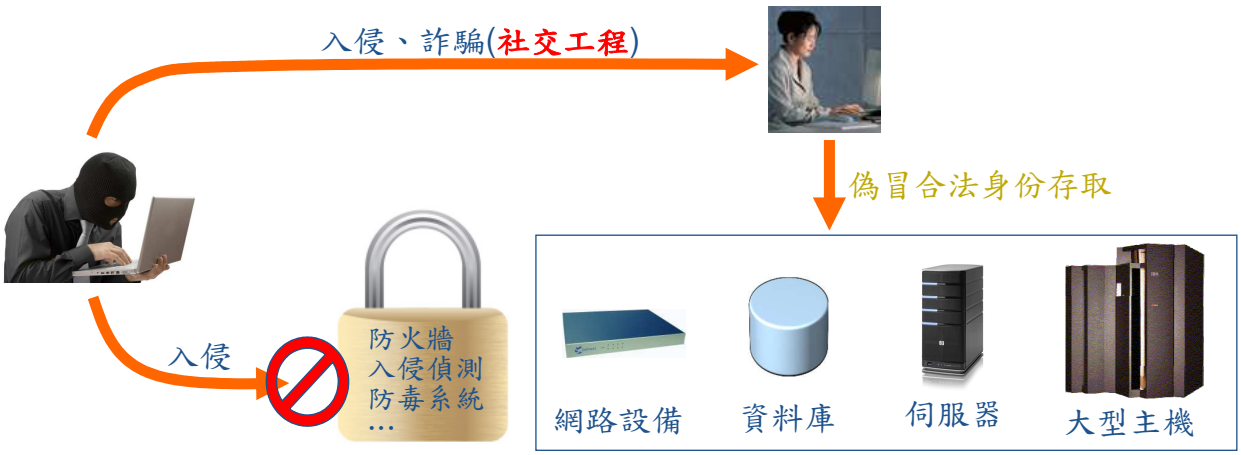


當你個資外洩時會發生什麼事？

詐騙集團可能會拿你的個資做的事情

資訊安全面面觀

- **The Security is as strong as the weakest link !**
  （系統安全強度＝ 最弱環節）



- 駭客攻擊順序
  - 先設法取得使用者的帳號、密碼
  - 再偽冒合法使用者登入重要主機、系統，進行竊密或破壞

課程大綱(Agenda)

- 本校資安宣導及推廣事項
- 從案例中探討資訊安全(含隱私權衝擊)
- 新冠肺炎疫情衝擊下資訊安全威脅(含資訊科技新知)
- 社交工程與案例分析(含勒索病毒+釣魚郵件)

2021面臨的資訊安全威脅

受疫情影響，遠距辦公、宅經濟、企業數位轉型成為流行趨勢，人們高度依賴網路的同時，也使資安風險不斷提升！專家預測，疫苗相關產業鏈、以疫情為契機針對企業與民間的攻擊、數位轉型伴隨的雲端風險、居家辦公帶來的家庭網路安全問題，將是2021年的資安攻防重點。

資安公司趨勢科技今日發表2021年資安預測報告，顯示至2020年第三季為止，已偵測、攔截到武漢肺炎相關威脅超過1300萬次，顯示疫情已成為今年駭客攻擊主軸，衍生手法包括網路釣魚、變臉詐騙等。

46

SafeLink 博創資訊

2021面臨的資訊安全威脅

變臉詐騙與網路釣魚

專家認為，今年疫情仍將是駭客最主要的誘餌。在企業方面，趁全球眾多公司持續遠距工作、許多事務難以當面確認之際，駭客可能透過變臉詐騙（Business Email Compromise，簡稱BEC）手法，假冒供應商寄郵件給員工，謊稱要變更銀行帳號或付款方式，誘使員工匯款。

在個人方面，則利用與疫情相關的資訊（例如申請政府失業補助、消滅病毒的方法等）散布釣魚郵件，引誘用戶點擊惡意連結或開啟惡意附件，進而竊取個資。

SafeLink – We Secure Your Network and Content.

2021面臨的資訊安全威脅

變臉詐騙(BEC)與網路釣魚

2021面臨的資訊安全威脅

變臉詐騙

BEC (Business Email Compromise) 商業電子郵件詐騙又稱為變臉詐騙，這是針對公務郵箱入侵、偽冒、潛伏觀察，再利用社交工程手法，誘騙公司或單位財務人員做轉帳匯款，造成巨額損失。這些精心設計的電子郵件，通常在前期透過釣魚 URL 或附件安插後門程式，在取得財務人員的郵箱密碼後，駭客持續觀察郵件往返內容直到出現大額轉帳信息時，偽造對方發送 BEC 變臉詐騙郵件，要求將該筆匯款轉到另外指定銀行帳戶。

SafeLink – We Secure Your Network and Content.

2021面臨的資訊安全威脅

趁疫入侵一字之差　台銀洛杉磯分行被騙走逾千萬元

臺銀海外分行因行員實施居家辦公，在家辦公的行員，收到一封電子郵件的匯款交易指示，因該行員居家無法做匯款交易，因此轉到分行去承做，但**分行也沒確認資料是否正確，就匯款出去了**。**事後核對後，發現電子郵件的地址中，有「一個字母」不同，主要是一個詐騙案**。

後來發現是因為隔了幾天，又有第二次匯款指示，行員驚覺跟客戶交易習慣不同，後來跟客戶確認，客戶才說沒有匯款指示，行員才驚覺第一次匯款遭騙。

變臉詐騙案例

2021面臨的資訊安全威脅

六個防止成為 BEC受害者防禦之道

- 仔細檢查所有的電子郵件。**小心來自高階主管送來的不尋常郵件**，因為它們是用來誘騙員工去緊急動作。**檢視要求資金轉移的電子郵件以確認該請求是否正常**。
- **教育和訓練員工**。雖然員工是公司最大的資產，當提到資訊安全，他們往往也是最脆弱的一環。提醒他們遵守組織政策是一回事，但養成良好的安全習慣是另一回事。
- **供應商付款位置改變要由組織人員進行第二層簽核來加以確認**。了解你客戶的習性，包括細節和付款背後的原因。
- **使用手機驗證來確認資金轉移請求以作為雙因子認證**，使用已知的熟悉號碼而非來自電子郵件中所提供的內容。
- 如果你懷疑自己成為BEC郵件的目標，立即向執法部門回報。

52

SafeLink 博創資訊

2021面臨的資訊安全威脅

疫情衝擊全球資安情勢
遠距辦公模糊家庭及工作界線 擴大資安防守範圍

值得注意的是，因疫情而衍生的混合辦公型態（例如每週僅一日進公司，其他時間在家上班），恐使家庭網路成為企業安全的潛在破口。

由於家庭網路缺乏企業網路的嚴密防護，專家預測，駭客可能會利用家庭網路漏洞對企業網路發動攻擊，或找到VPN網路中具有關鍵數據或企業機密的目標，進一步攻擊以竊取企業機密，對此，零信任模式 (Zero Trust) 將在2021年成為企業安全策略關鍵點之一，如何落實安全存取可視性及提升訪問資料的管理權限將為企業防禦佈局重點。

53

SafeLink – We Secure Your Network and Content.

2021面臨的資訊安全威脅

遠距工作時網路安全10大要點

企業端守則

1. 多人同時應用遠端連線，同時非上班時間也會出現更多支援需求。此時，網路頻寬、資料貯存能力、以及運算效能受到考驗。儘管信息流量增加了，對於細節也還是不能馬虎。企業應更加留意這些需求，並做好資源分配計畫。
2. 使用最新的網路、遠端連線應用程式易受入侵，它很有可能是意圖不軌份子趁虛而入竊取重要機密的環節。因此，應使用最新的軟體和資安補強措施，防堵任何已知漏洞。
3. 企業應該整合本身的持續營運計畫、災後復原計畫、以及資安事件應變計畫。不肖份子知道，更多人遠端連線，企業會特別仰賴網路架構以及網路暢通，他們也會利用這個狀況竊取資料。
4. 密切監控任何必要的權限開放措施，企業可能會需要開放一些公開的資安政策、標準、或實務守則當中所規定的權限。針對這些例外作為，要進行詳細的評估過程、並且要嚴密的監控。
5. 採用多重要素驗證，傳統用戶使用的登入及密碼帳號，很容易遭到不肖份子入侵。可能的話，身分驗證設定多重要素驗證程序(multi factor authentication)，如此可以幫助您建立對抗網路犯罪的第二道防線。

54

2021面臨的資訊安全威脅

使用端守則

1.任何您在網路上或者透過行動通訊應用程式分享的資訊，都可能被他人取得。所以一定要**使用虛擬私人網路來確保安全的遠距工作連線**。利用個人的電腦或手機進行遠距辦公時，**務必只使用加密的企業虛擬私人網路連線通道**。

2.許多人在每個網站都使用同一組或者相似的密碼、甚至辦公室和家中的密碼也沒有區別。但是，這意味著駭客只要竊取一組密碼，就能夠在好幾個網站上解鎖許多個帳號的資料。**因此，每個帳號使用安全且複雜的密碼較為安全。亦或使用密碼管理軟體確保您在每個網站或服務上能使用較為複雜、難以破解的密碼**。

3.**只在信任的網站或者郵件中點擊連結、開啟附件、或者下載軟體**。不肖份子利用這傳送夾帶似乎有用資訊的連結。一旦點擊了，不肖分子就能利用這個惡意連結來取得個人或者企業的機密資訊。

4.分享機密資訊之前，先驗證網址。不肖份子會創立一個非常擬真的詐騙網頁，**所以不要使用電子郵件中所附的連結，而要直接使用鍵盤輸入網址來連結信任的網站**。此外，要確定您所造訪的網頁網址當中含有HTTPS；這類的網站比網址中含有 HTTP的網站更安全。

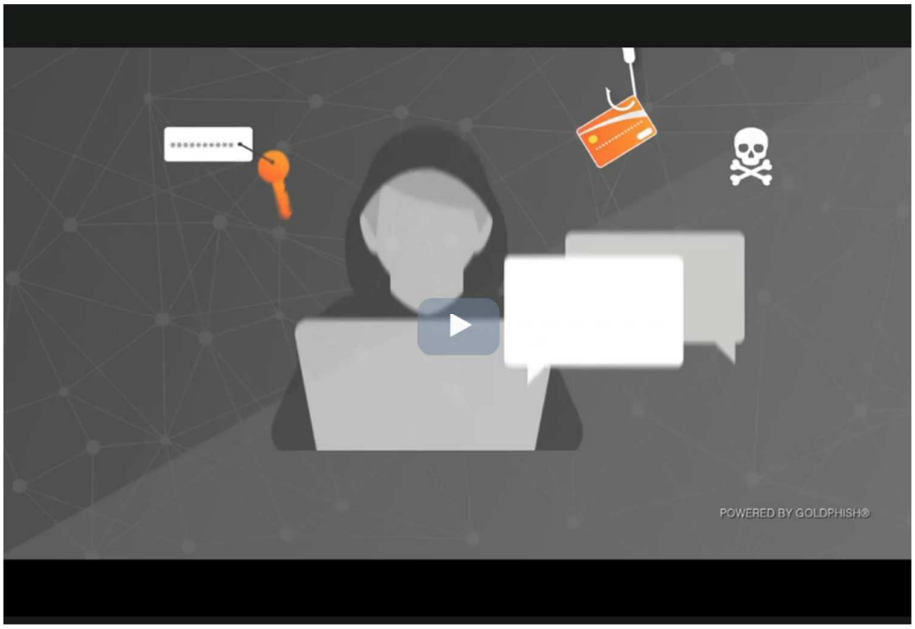
5.不要回覆不明來源提出的資訊要求—特別提出與個人身分有關的資訊或密碼的要求不肖分子會試圖假冒成您認識的人或者同事來誘騙人們分享機密資訊。

SafeLink – We Secure Your Network and Content.

課程大綱(Agenda)

- 本校資安宣導及推廣事項
- 從案例中探討資訊安全(含隱私權衝擊)
- 新冠肺炎疫情衝擊下資訊安全威脅(含資訊科技新知)
- 社交工程與案例分析(含勒索病毒+釣魚郵件)

社交工程詐騙-電子郵件篇



駭客入侵實錄-電子郵件篇

影片中，您看到了那些造成資安事件的問題？

APT 針對性攻擊

- **APT（Advanced Persistent Threats）**
  - 針對特定組織進行的多方位網路攻擊
  - 過去APT多以政府為目標，尤其是政治動盪的區域，前年開始針對企業或大型組織，擁有越多用戶資料的網站越是駭客眼中的大肥羊
- **APT特性**
  - 多半不直接攻擊提供外部服務主機(如官方網站)的弱點
  - 常以電子郵件搭配惡意檔案，透過社交工程進行攻擊
  - 惡意檔案多透過文件檔案進行包裹，如PDF、XLS、DOC等
  - 感染目標組織的主機後，不立即進行大規模破壞或擴散、不佔用太多主機資源，網路使用量也低，可長期潛伏不易發現
  - 惡意程式的活動、攻擊、擴散皆具目標性

SafeLink – We Secure Your Network and Content.

社交工程定義

- 社交工程是利用人性的弱點(貪心、好奇心...)或人際之信任關係進行詐騙，是一種非「全面」技術性的資訊安全攻擊方式。(例如藉由電話、電子郵件或假扮身分來進行社交工程)
  - 不須高深的資訊技術即可獲取帳號、密碼、信用卡密碼、身分證號碼、姓名、地址或其他身分或機密資料的方法。
  - 就算擁有高科技的資安設備、高效能的防護系統，只要需要人為操作，就有遭受社交工程攻擊的危機。

60

SafeLink 博創資訊

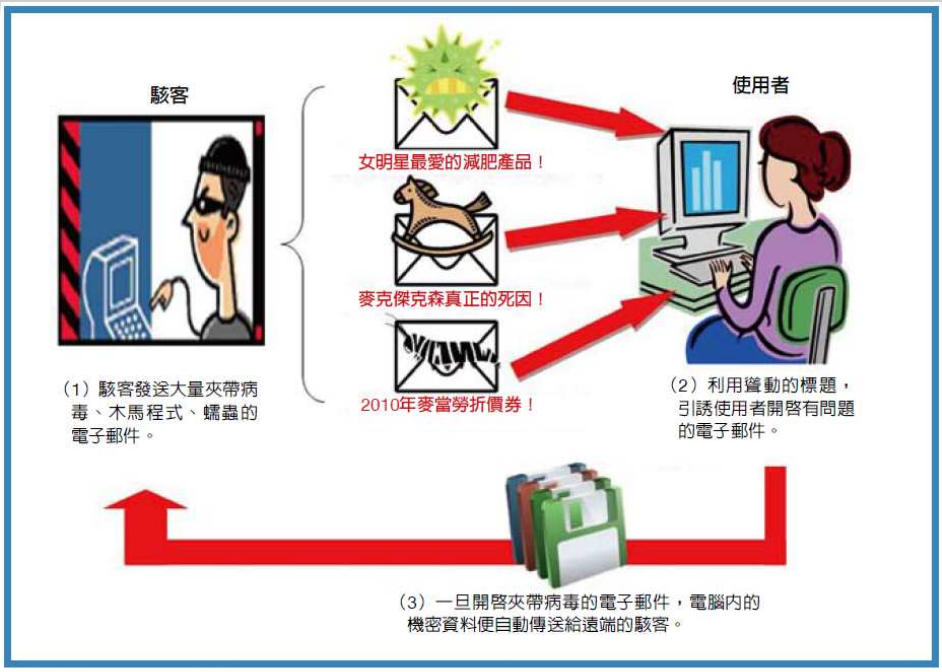
社交工程－攻擊目的

- 竊取機密檔案/文件
- 針對性資料蒐集(企業商業機密[新研發產品])
- 線上遊戲之有價財產(遊戲寶物)
- 部落格或社群網站之帳號密碼
- 工作商業機密資料
- 跳板(殭屍電腦)
- 監控使用者行為
- 智慧型手機使用者個資(通訊錄、E-Mail等)

社交工程攻擊管道與手法

- 電話詐騙(早期的攻擊管道)
- 電子郵件隱藏惡意程式
- 網路釣魚
- 圖片中的惡意程式
- 偽裝修補程式
- 軟體弱點與零時差攻擊
- USB隨身碟
- 即時通訊軟體也成為傳播惡意程式的途徑
  - LINE
  - SKYPE

社交工程－電子郵件隱藏惡意程式



利用電子郵件進行社交工程的過程

社交工程－釣魚郵件的內容特性

- 令人緊張或鬆懈防備之郵件
  - 關心提醒(請告訴身旁的女性朋友，小心電梯之狼)
  - 誇大聳動(世界末日大預言)
  - 郵件回覆(RE:會議參考資料)
  - 郵件轉寄(FW:簡易規劃日本自助)
- 工作業務、生活時事等相關或令人感興趣之郵件內容類型
  - 政治新聞、特殊新奇
  - 生活議題、休閒娛樂
  - 社交群體、健康養生

社交工程－電子郵件隱藏惡意程式

另人好奇的
郵件主旨

健康類_長途旅遊慎防下肢血栓_TANET
新奇類_免費停車場卻被收100_TANET
旅遊類_大阪五處必逛景點_TANET
新奇類_免費停車場卻被收100_TANET
旅遊類_大阪五處必逛景點_TANET
旅遊類_少女峰雪景超夢幻_TANET
健康類_吃素一年反而加重脂肪肝_TANET
健康類_長途旅遊慎防下肢血栓_TANET
健康類_長途旅遊慎防下肢血栓_TANET
健康類_長途旅遊慎防下肢血栓_TANET
旅遊類_大阪五處必逛景點_TANET
旅遊類_大阪五處必逛景點_TANET
旅遊類_少女峰雪景超夢幻_TANET
旅遊類_大阪五處必逛景點_TANET
科技類_體驗混合實境_TANET
健康類_吃素一年反而加重脂肪肝_TANET

65

SafeLink – We Secure Your Network and Content.

社交工程－電子郵件隱藏惡意程式

吸引人的
郵件主旨

公務類_公務員懲戒新制實施_tanet
公務類_公務員廉政倫理規範_tanet
時事類_「政黨民主」與「民心」真正的距離_tanet
公務類_公教人員年終工作獎金發給注意事項_tanet
公務類_公教人員年終工作獎金發給注意事項_tanet
公務類_公教人員年終工作獎金發給注意事項_tanet
公務類_公務員廉政倫理規範_tanet
公務類_公務員廉政倫理規範_tanet
健康類_喝咖啡易得食道癌？_tanet
公務類_公務員廉政倫理規範_tanet
健康類_喝咖啡易得食道癌？_tanet
公務類_公教人員年終工作獎金發給注意事項_tanet
公務類_公教人員年終工作獎金發給注意事項_tanet
公務類_公務員廉政倫理規範_tanet
公務類_公務員廉政倫理規範_tanet

SafeLink 博創資訊

社交工程－釣魚郵件的內容特性

一、信件主旨：小7無人商店開放第一天記者實際體驗；結帳只要10秒

二、信件主旨：2018國民旅遊卡特約商店優惠方案

67

SafeLink – We Secure Your Network and Content.

社交工程－釣魚郵件的內容特性

三、信件主旨：2019最夯燒肉丼排行榜，爆量肉山讓人看了直流口水

四、信件主旨：東京迪士尼投下2500億建新3大園區！冰雪奇緣&彼得潘區2022年開幕！概念圖預覽

68

SafeLink 博創資訊

社交工程－釣魚郵件的內容特性

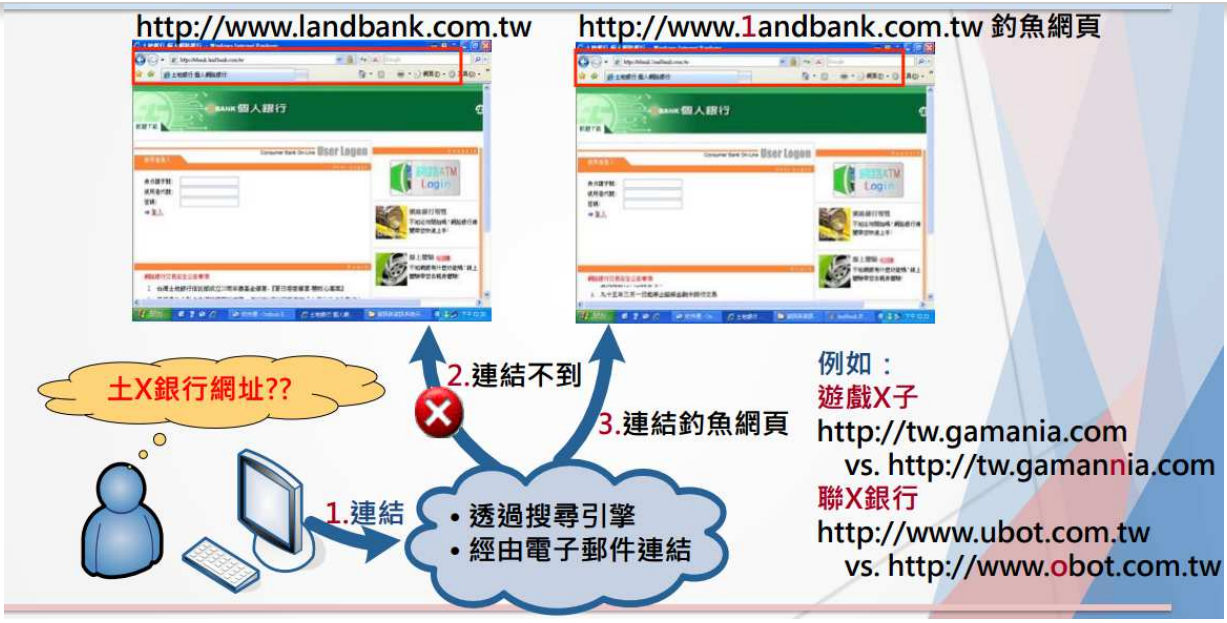
五、信件主旨：你填問卷，抽週週Switch及百種遊戲片

六、信件主旨：公務人員健康檢查之醫院有何規定？

69

SafeLink – We Secure Your Network and Content.

釣魚郵件案例(1)-偽造銀行網站



偽造網址：http://www.landbank.com.tw
偽造網站竊取受害者網路銀行登入帳號與密碼

資料來源：趨勢科技

釣魚郵件案例(2)-仿冒中華電信寄帳單

71

釣魚郵件案例(3)-偽裝政府機關

釣魚郵件案例(4)-冒牌網站

- 駭客註冊網域名稱與「正牌」網站極為相似

www.landbank.com.tw	www.1andbank.com.tw
www.104.com.tw	www.1O4.com.tw
www.bot.com.tw	www.b0t.com.tw
www.acer.com.tw	www.accer.com.tw

真 假

社交工程－惡意程式

- 社交工程惡意程式專門假冒其他軟體和/或隱藏在其他軟體之內，引誘使用者下載並安裝該軟體，藉此趁機安裝惡意軟體。社交工程惡意程式不論對個人或對公司都會造成嚴重的風險，進而導致機密資訊遭盜用竊取、損毀或外流。
- 目前經由網頁感染的惡意程式佔所有惡意程式的50% 以上，因此這類威脅必須透過更精良的技術和資源以及使用者正確的資訊安全素養來防範。

74

社交工程－網路釣魚 Part I

75

釣魚郵件案例(1)-偽造銀行網站

近期詐騙集團開始愛用【手機簡訊】的方式進行詐騙，訊息內容例如「有包裹待領」、「銀行帳戶異常」等等，通常這些簡訊都會附上一個「魚目混珠」的短網址，讓人難辨真假。

**趨勢科技防詐達人:可將簡訊轉貼到LINE上面「防詐達人」做進一步查驗。另外若發現在該銀行登入頁，隨便輸入帳號密碼，卻依舊可以通過，就是假的。

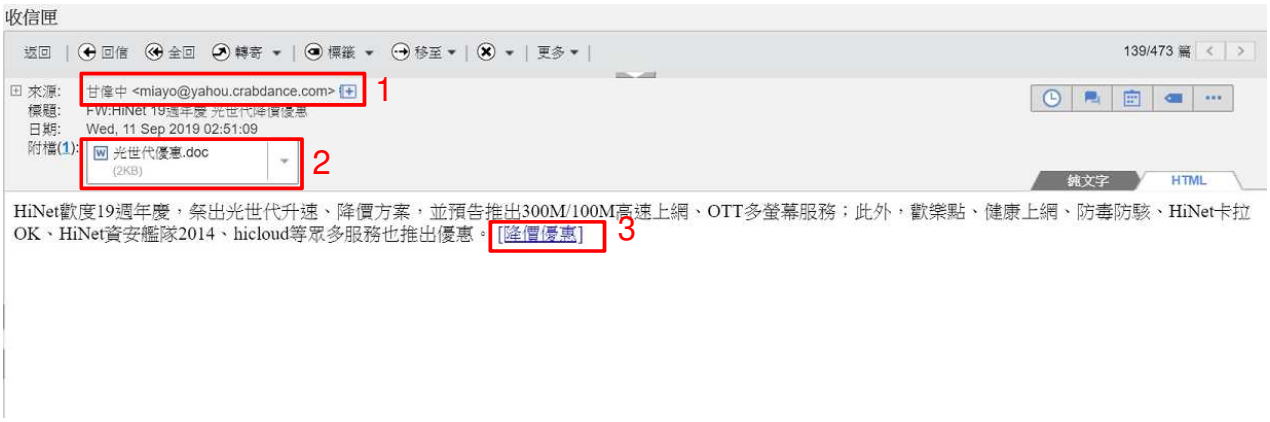
SafeLink 博創資訊

釣魚郵件案例(2)-仿冒中華電信寄帳單

點選附件下載通話費明細

SafeLink – We Secure Your Network and Content.

釣魚郵件案例(3)



SafeLink 博創資訊

釣魚郵件案例(4)-冒牌網站

- 駭客註冊網域名稱與「正牌」網站極為相似

www.landbank.com.tw	www.1andbank.com.tw
www.104.com.tw	www.1O4.com.tw
www.bot.com.tw	www.b0t.com.tw
www.acer.com.tw	www.accer.com.tw

真

假

社交工程測試宣導(1)

- 電子郵件社交工程測試演練宣導
  - 受測人員寄發 10 封測試測試信件進行統計分析作業，統計**受引誘而預覽信件、連結點選或開啟附檔之數量及比率**。
  - 測試信件**寄件人名稱，均為偽造**，用來測試受測人對寄件人名稱是否合理的辦識能力。

社交工程測試宣導(2)

一、 測試成功定義

（一）開啟信件：信件透過預覽或點開方式開啟，且信件本文內所含圖片亦完成圖片下載之動作，始認定為測試成功。以教育部員工使用郵件系統，其預設之安全設定不會自動下載圖片，即使預覽功能設定為開啟，或是直接打開測試信件，因無下載圖片之動作，不會造成安全漏洞，將不會記錄為測試成功。

（二）點選連結：受測人員點選信件內文中之連結網址，將被記錄為測試成功。

（三）開啟附檔：受測人員開啟信件內文中之附檔，將被記錄為測試成功。

社交工程的預防

- 隨時具備危機意識，對於任何詢問重要資料的人士，都需小心求證(防制詐騙中心)
- 單位內對權限應加以分級控管，非屬個人分內事宜，不應掌握帳號、密碼等特殊權限，防止因不了解安全等級而不慎外流重要資料
- 安裝防毒軟體，設定個人防火牆，並定期更新病毒碼
- 針對電腦應用程式應隨時更新修補程式；設定安全密碼（6~8碼，包括英數與符號字元），避免太簡單易遭破解的密碼
- 重要資料檔案要加密防護(WORD、Excel)

社交工程－電子郵件安全使用概念

- 來路不明的超連結勿點選
- 嚴格把關附件開啟動作(注意副檔名[.exe])
- 關閉郵件預覽功能(outlook express)
- 不自動下載HTML電子郵件訊息或RSS項目中的圖片
- 檢視收件者清單(是否為群組發送)
- 檢視寄件者(是否業務相關?是否認識?)

對抗APT.預防勒索病毒(APT)1

資料來源：趨勢科技

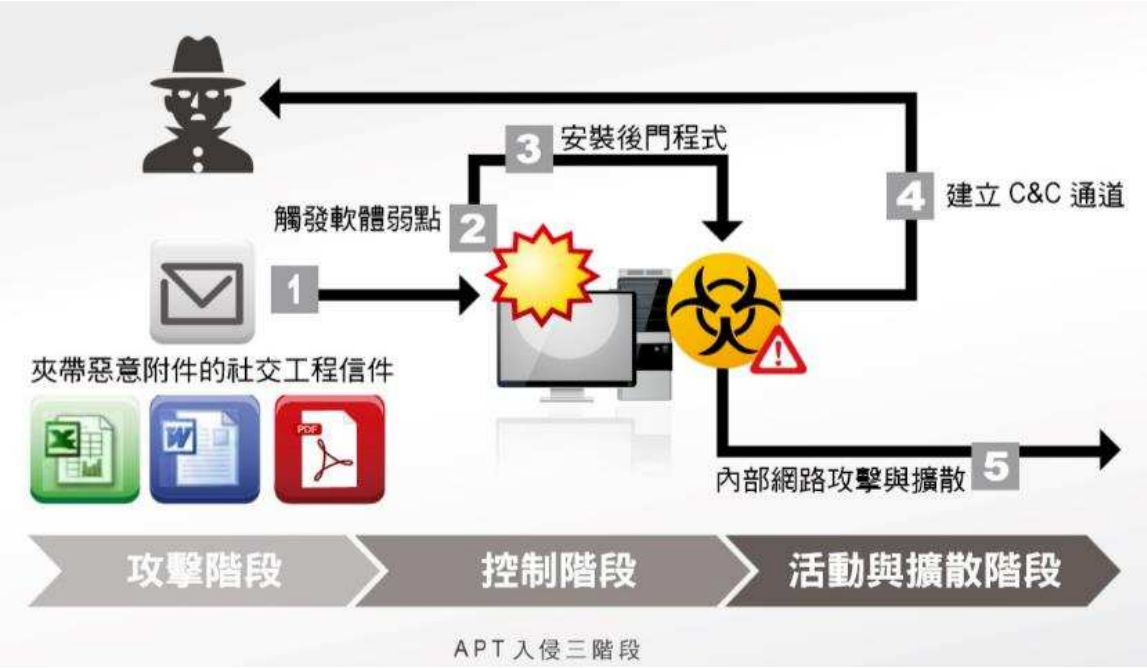
APT進階持續性滲透攻擊(APT)2

APT攻擊流程

鎖定目標	• 背後通常有豐沛資源或組織支援，亦有針對性目標與範疇，如國防、重要機關、金融及學術界等
收集資訊	• 透過各種公開或地下的管道進行資料收集，包括公開或機密資訊，社群網站、端點防禦設備、網路架構等
攻擊滲透	• 根據收集資訊來規劃設計攻擊策略
建立據點	• 滲透成功後，開啟後門取得控制權並持續滲透攻擊，躲避防毒機制偵測
分析資訊	• 透過監聽、網芳攻擊及檔案伺服器，以蒐集並分析內部機密資訊，如帳密、網路架構機密文件
權限提昇	• 提昇於系統主機或伺服器之權限
回傳機密資料	• 打包並回傳機密資料
消除系統紀錄	• 消除系統主機或伺服器之相關紀錄

APT進階持續性滲透攻擊(APT)3

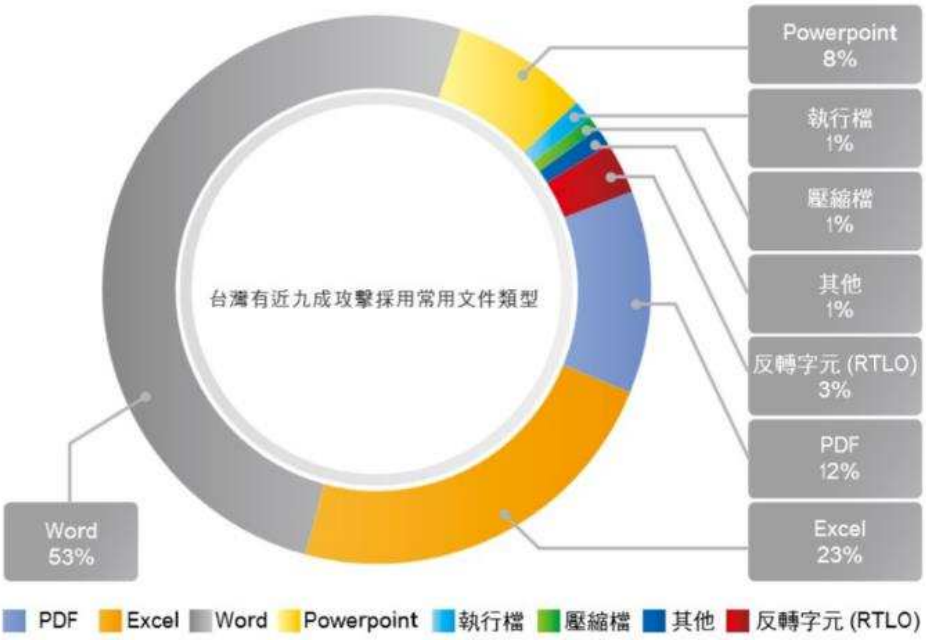
- APT 入侵 三 階 段



資料來源：趨勢科技APT威脅白皮書

APT進階持續性滲透攻擊(APT)4

- APT電子郵件社交工程攻擊常用文件類型



資料來源：趨勢科技APT威脅白皮書

SafeLink – We Secure Your Network and Content.

你該有的危機意識

- 詐騙網站防不慎防，不要以為你有裝防毒軟體，或是使用有惡意網站阻擋功能的瀏覽器 (比如 Google Chrome 提供 Safe Browsering)，就覺得安全囉！現有的防護機制還是以黑名單為主，當瀏覽器或防毒軟體發現你瀏覽的網站有問題時，會給你一個大大的警告，阻止你繼續瀏覽。
- 可是新的詐騙網站上線後，通常要經過一段時間才會被資安單位發現並加入黑名單，這之中的空窗期就變得相當危險，壞人可能透過電子郵件的方式散播，用很聳動的標題騙你打開，或是在你瀏覽網頁時彈出新視窗，比如「恭喜中大獎」之類的畫面。

Q&A 問題與討論

～如有任何問題，歡迎隨時來電詢問～

SafeLink
博創資訊科技股份有限公司
臺中市西屯區國安一路208巷6號
TEL：(04)2525-0535
FAX：(04)2461-5268
http://www.safelink.com.tw/
E-mail: sam@safelink.com.tw

課後評量測驗

課名: 111年第1梯次資通安全通識教育訓練

測驗卷網址及QRCode:

https://forms.gle/pi7sdudF6vLXLMvt7