TSC CAPITAL GROUP
The Bridge to the Asia Pacific Region

國立臺南大學

111年資訊安全暨個人資料管理規範導入顧問輔導服務案
課程名稱：個人資料保護與管理認知

授課日期：111年7月13日
授課講師：德欣寰宇科技股份有限公司 資安顧問 吳懿仁

簡報大綱

一 個人資料保護法介紹

二 個資保護基本認知及社交工程結果說明

三 案例分享與討論

四 課程總結

tsc 淘邦 TSC CAPITAL GROUP The Bridge to the Asia Pacific Region

個人資料保護法介紹

tsc 德邦 TSC CAPITAL GROUP
The Bridge to the Asia Pacific Region

個人資料保護法歷程

84年

- 公布［電腦處理個人資料保護法］

99年

- 公布「個人資料保護法」

101年

- 公布［個人資料保護法］施行

104年

- 公布修正之「個人資料保護法」部分條文

105年

- 修正之「個人資料保護法」部分條文施行

有限適用範圍 → 全面適用

tsc 海外 TSC CAPITAL GROUP
The Bridge to the Asia Pacific Region

個人資料保護法架構

第一章 總則(§1~§14)

第二章
公務機關對個人資料之蒐集、處理及利用
(§15~§18)

第三章
非公務機關對個人資料之蒐集、處理及利用
(§19~§27)

第四章
損害賠償及團體訴訟
(§28~§40)

第五章
罰則
(§41~§50)

第六章
附則
(§51~§56)

tsc 遠東 TSC CAPITAL GROUP
The Bridge to the Asia Pacific Region

個人資料保護法立法目的§1

規範個人資料之蒐集、處理及利用

避免人格權受侵害

促進個人資料合理使用

何謂個資?

一般個資§2

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、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。

特種個資§6 I

病歷、醫療、基因、性生活、健康檢查、犯罪前科

特種個資定義-個資法施行細則§4

類別	對應個資法	內容定義
醫療 (C111健康紀錄)	醫療	指以治療、矯正或預防人體疾病、傷害、殘缺為目的 ，所為的診察、診斷及治療；或基於診察、診斷結果，以治療為目的，所為的處方、用藥、施術或處置等行為全部或一部之總稱。
	病歷	依醫療法第六十七條所定之病歷應包括下列各款之資料： 一、醫師依醫師法執行業務所製作之**病歷**。 二、各項檢查、檢驗報告資料。 三、其他各類醫事人員執行業務所製作之紀錄。
基因 (C113種族或血統來源)	基因	指由人體一段去氧核醣核酸(DNA)構成，為人體控制特定功能之遺傳單位訊息。
性生活 (C112兩性生活)	性生活	指所有與性行為有關之活動之總稱，如性傾向、性慣行等。
身心健康狀況 (C66健康與安全紀錄) (C111健康紀錄)	健康檢查	指非針對特定疾病進行診斷或治療之目的，而以醫療行為施以檢查所產生之資料，如**健康檢查報告、身心輔導報告**等。
犯罪前科 (C115其他裁判及行政處分)	犯罪前科	指經緩起訴、職權不起訴或法院判決有罪確定、執行之紀錄。

個資法所指行為定義 §2

個資法所指行為定義

蒐集	指以任何方式取得個人資料
處理	指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送
利用	將蒐集之個人資料為處理以外之使用
國際傳輸	將個人資料作跨國（境）之處理或利用

tsc 海邦 TSC CAPITAL GROUP The Bridge to the Asia Pacific Region

當事人對自身個資之權利-個人資料保護法§3

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。

§13/ §10
15Day+15Day

§13/ §10
30Day+30Day

書面告知
延長原因

可拒絕當事人行使權利情形

一、妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。
二、妨害公務機關執行法定職務。
三、妨害該蒐集機關或第三人之重大利益。

tsc 遠東 TSC CAPITAL GROUP
The Bridge to the Asia Pacific Region

合理且適當使用個資-個人資料保護法§5

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。

【疾管署忙防疫遭駭3】為查志玲姐姐懷孕沒？ 台大醫護偷查病歷被抓包

鏡週刊Mirror Media | 19.3k 人追蹤 追蹤

林俊宏
2020年4月29日 上午5:

警察偷查IG正妹個資　賠50萬求和解失敗遭起訴

編輯 陳儷文 報導 2019/10/29 20:32

小 中 大

網傳上海公安系統遭駭 10億公民個資售20萬美元

The Central News Agency 中央通訊社
2022年7月4日

（中央社台北4日電）中國網路瘋傳疑似發生大規模的個資外洩案，近日有駭客在某論壇上猖狂放話稱，出售上海公安系統數據庫，「包含10億中國公民的訊息，以20萬美元出售」，目前中國官方未有證實和回應。

「星島日報」今天報導，6月30日上午有位帳號名為「ChinaDan」的網友在某論壇發布消息稱：「上海國家警察數據庫（SHGA.gov.cn）遭到洩露，數據詳情有10億中國國民居民訊息和數十億病例記錄，包括姓名、地址、出生地、身分證、手機號碼及所有犯罪/案件詳情。」

tsc 遠東 TSC CAPITAL GROUP The Bridge to the Asia Pacific Region

特種個人資料之蒐集、處理及利用-個人資料保護法§6

有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：

- 一、法律明文規定。
- 二、公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施
- 三、當事人自行公開或其他已合法公開之個人資料。
- 四、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。
- 五、為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。
- 六、經當事人書面同意。但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集處理或利用，或其同意違反其意願者，不在此限。

依前項規定蒐集、處理或利用個人資料，準用第八條、第九條規定；其中前項第六款之書面同意，準用第七條第一項、第二項及第四項規定，並以書面為之。

當事人同意-個人資料保護法§7

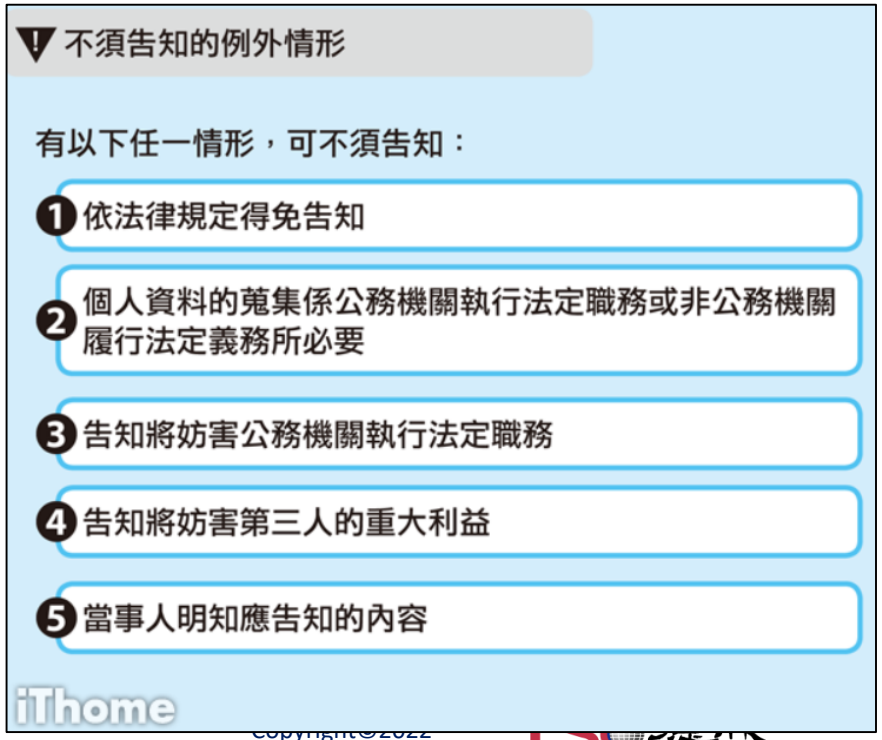
- 第十五條第二款及第十九條第一項第五款所稱同意，指當事人經蒐集者告知本法所定應告知事項後，所為允許之意思表示。
- 第十六條第七款、第二十條第一項第六款所稱同意，指當事人經蒐集者明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響後，單獨所為之意思表示。
- 公務機關或非公務機關明確告知當事人第八條第一項各款應告知事項時，當事人如未表示拒絕，並已提供其個人資料者，推定當事人已依第十五條第二款、第十九條第一項第五款之規定表示同意。
- 蒐集者就本法所稱經當事人同意之事實，應負舉證責任。

告知當事人義務-個人資料保護法§8

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

如果是間接收集個資(非當事人提供)，需向當事人告知上述**第一項至第五項**所列事項。(個人資料保護法§9)



蒐集目的與個人資料類別(補充說明)

- 法務部於民國101年正式對外公告個資法的特定目的及個人資料類別，特定目的有182 項，而個資類別有10 大類共134 項，這些是為了提供公務和非公務機關在個資蒐集、處理和利用時，衡量「符合特定目的內的利用」時的重要參考依據。

中華民國 法務部 Ministry Of Justice

主管法規查詢系統 Laws and Regulations Retrieving System

代號	特定目的項目
〇〇一	人身保險
〇〇二	人事管理（包含甄選、離職及所屬員工基本資訊、職、學經歷、考試分發、終身學習訓練進修、考績懲、銓審、薪資待遇、差勤、福利措施、褫奪公權殊查核或其他人事措施）
〇〇三	入出國及移民
〇〇四	土地行政
〇〇五	工程技術服務業之管理
〇〇六	工業行政
〇〇七	不動產服務
〇〇八	中小企業及其他產業之輔導
〇〇九	中央銀行監理業務
〇一〇	公立與私立慈善機構管理
〇一一	公共造產業務
〇一二	公共衛生或傳染病防治
〇一三	公共關係
〇一四	公職人員財產申報、利益衝突迴避及政治獻金業務
〇一五	戶政
〇一六	文化行政

代　號	識別類：
C〇〇一	辨識個人者。 例如：姓名、職稱、住址、工作地址、以前地址、住家電 碼、行動電話、即時通帳號、網路平臺申請之帳號、通訊 籍地址、相片、指紋、電子郵遞地址、電子簽章、憑證卡 、憑證序號、提供網路身分認證或申辦查詢服務之紀錄及 任何可辨識資料本人者等。
C〇〇二	辨識財務者。 例如：金融機構帳戶之號碼與姓名、信用卡或簽帳卡之號 保險單號碼、個人之其他號碼或帳戶等。
C〇〇三	政府資料中之辨識者。 例如：身分證統一編號、統一證號、稅籍編號、保險憑證 、殘障手冊號碼、退休證之號碼、證照號碼、護照號碼等

代　號	特徵類：
C〇一一	個人描述。 例如：年齡、性別、出生年月日、出生地、國籍、聲音等
C〇一二	身體描述。 例如：身高、體重、血型等。
C〇一三	習慣。 例如：抽煙、喝酒等。
C〇一四	個性。 例如：個性等之評述意見。

告知當事人方式-個人資料保護法施行細則§16

依本法第八條、第九條及第五十四條所定告知之方式，得以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。

安全維護事項-個人資料保護法施行細則§12

本法第六條第一項但書第二款及第五款所稱適當安全維護措施、第十八條所稱安全維護事項、第十九條第一項第二款及第二十七條第一項所稱適當之安全措施，指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施。

Plan

1. 配置管理之人員及相當資源
2. 界定個人資料之範圍
3. 個人資料之風險評估及管理機制
4. 事故之預防、通報及應變機制
5. 個人資料蒐集、處理及利用之內部管理程序

Do

6. 資料安全管理及人員管理
7. 認知宣導及教育訓練
8. 設備安全管理

Check

9.資料安全稽核機制
10.使用紀錄、軌跡資料及證據保存

Action

11.個人資料安全維護之整體持續改善

個資法施行細則§12-安全維護事項(1/2)

一、配置管理之人員及相當資源:成立個資保護組織（個資管理委員會）、設置個資保護聯繫窗口並指定各單位個資保護專人、提供足夠之個資保護資源及承諾。

二、界定個人資料之範圍：個資盤點清查(紙本、電子檔案、系統)

三、個人資料之風險評估及管理機制：需進行個資風險評估，並對違法事項或高風險項目訂定風險處理計畫

四、事故之預防、通報及應變機制：事故發生時包含內部通報、主管機關通報、當事人的權益通報程序、應變處理程序都應該明訂。

五、個人資料蒐集、處理及利用之內部管理程序：應訂定及實施個人資料蒐集、處理及利用之內部管理程序。

六、資料安全管理及人員管理：應建立及實施個人資料保護管理機制及人員安全管理。

個資法施行細則§12-安全維護事項(2/2)

七、認知宣導及教育訓練：應辦理個資認知宣導及相關專業訓練。

八、設備安全管理：主要是針對各種保存個資的設備或系統，應該要做完善的安全保護（資訊安全作業）。

九、資料安全稽核機制：應定期實施個資安全稽核。99年8月份法務部函文政風單位須將個資檢查納入年度內稽。

十、使用紀錄、軌跡資料及證據保存： IT設備或紙本資料個資存取、使用、流向的記錄、日誌檔（Log）等，都必須完整保留，因為這些都是舉證的證據力(善盡保管之責任)。

十一、個人資料安全維護之整體持續改善：針對個資保護不足之處持續更新(PDCA)。

（補充說明）使用紀錄、軌跡資料及證據保存(1/2)

個資使用紀錄、軌跡資料即證據保存分類可分為以下三類:

個資當事人權利紀錄

1.告知義務及當事人同意之紀錄。
2.當事人行使權利之紀錄或切結書。
3.准駁當事人行使權利之紀錄。
4.個資事件發生時通知當事人之紀錄。

內部處理紀錄

1.ISMS&PIMS施行紀錄。
2.實體安全控制紀錄。
3.設備安全管制紀錄。
4.人員安全管理紀錄。
5.資料安全管理紀錄。
6.委託管理紀錄。

軌跡資料

1.安全控管設備運作。
2.網路軌跡。
3.資料庫軌跡。
4.具備特殊權限帳號之存取行為軌跡。
5.存取權限異動軌跡。
6.電子郵件軌跡。
7.存取個資檔案軌跡

（補充說明）使用紀錄、軌跡資料及證據保存(2/2)

應用系統留存軌跡資料(log)有助於日後事件追查，下表提供參考。

NO	欄位名稱	說明
1	系統登入IP	記錄系統連線的IP 位址
2	使用者代號	使用者登錄代號
3	登入時間	使用者登入系統時間
4	執行程式代號	執行程式的代號
5	程式執行時間	程式開始執行的時間
6	處理動作	查詢/新增/修改/刪除/複製……
7	異動內容	查詢或異動的內容(可記錄異動的資料主鍵值)
8	程式結束時間	執行程式結束的時間
9	系統登出時間	結束系統登出的時間

試著思考看看...當您管理的資通系統發生個資洩漏，
比對的出來人、事、時、地、物嗎？

個人資料保護法§12-個資事件發生後通知當事人

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。

親愛的消費者/會員您好：

非常抱歉，（公司或網站名稱）因（原因）發生個人資料外洩事故，且已有消費者接獲詐騙集團電話。提醒您，詐騙集團通常於週末或下班時間以（手法）誆騙消費者。如接獲疑似詐騙電話，請不要聽從指示操作 ATM 或提供任何個人資料，並立即通報 165 警政署反詐騙專線。

針對這次事件，本公司已（改善措施），未來也會持續加強資訊安全與個人資料保護管理，以降低消費者個資被侵害之風險。

如有關於訂單或本次個資事故之疑問，請於（上班時間）與本公司客服人員聯絡（電話）；上班時間以外請以（提供其他可行方式）聯絡本公司。

（公司名稱）　敬上

通知資訊3重點！！！！！
1.個資當事人個人資料被侵害之事實
2.已採取之因應措施(處理情形)
3.後續供當事人查詢之專線與其他查詢管道

tsc 遠東 TSC CAPITAL GROUP The Bridge to the Asia Pacific Region

個人資料保護法施行細則§22-適當方式通知當事人

第 22 條　1　本法第十二條所稱適當方式通知，指即時以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。但需費過鉅者，得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之。

2　依本法第十二條規定通知當事人，其內容應包括個人資料被侵害之事實及已採取之因應措施。

銓敘部個資外洩通知

本部於108年6月22日接獲外部情資知悉國外網站揭露疑似本部所掌理之個人資料餘59萬筆，本部依個人資料保護法第12條及施行細則第22條規定通知當事人相關事項如下：

一、影響範圍：94年1月1日至101年6月30日間中央及地方機關公務人員送審人員歷史資料，實際影響人數為243,376筆，欄位包含身分證字號、姓名、服務機關、職務編號、職稱。

二、已採取因應措施：

(一) 依資通安全管理法向行政院國家資通安全會報技術服務中心進行資安事件通報。

(二) 疑似外洩資料之資訊系統早已於104年3月下線，為求審慎，本部即刻對本案現行運作相關資通系統進行弱點檢測及重新檢視防護措施。

針對本事件，本部已協請行政院資通安全處協助進行根因調查及全機關全面性資通安全檢測，本部將確實檢討改進，並依資通安全管理法及個人資料保護法持續精進各項資通安全及個資保護相關作為。

銓敘部108年個資外洩事件

tsc 遠航 TSC CAPITAL GROUP The Bridge to the Asia Pacific Region

公務機關對個資之蒐集、處理§15

- 公務機關對個人資料之蒐集或處理，除特種資料外，應有 特定目的，並符合下列情形之一：

  -執行法定職務必要範圍內。

  -經當事人同意。

  -對當事人權益無侵害。

公務機關對個資之利用§16

公務機關對個人資料之利用，除特種資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。但有下列情形之一者，得為特定目的外之利用：

- 法律明文規定。
- 為維護國家安全或增進公共利益所必要。
- 為免除當事人之生命、身體、自由或財產上之危險。
- 為防止他人權益之重大危害。
- 公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。
- 有利於當事人權益。
- 經當事人同意。

不適用個資法情況

個資法 第51條
有下列情形之一者，不適用個資法規定

自然人為單純個人或家庭活動之目的，而蒐集、處理或利用個人資料。

於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料。

tsc 遠東 TSC CAPITAL GROUP
The Bridge to the Asia Pacific Region

個資保護基本認知及社交工程結果說明

個人資料蒐集之基本管控重點

- 個資蒐集不逾越特定目的。
- 個資蒐集須符合個資法有關蒐集之法定要件。
- 個資蒐集須履行當事人之告知義務。

個人資料提供同意書

文件編號：NUTN-PIMS-D016	版次：1.0	機密等級：一般
紀錄編號：	填表日期：　年　月　日	

本同意書說明國立臺南大學（以下簡稱本校）將如何處理本表單所蒐集到的個人資料。當您勾選「我同意」並簽署本同意書時，表示您已閱讀、瞭解並同意接受本同意書之所有內容及其後修改變更規定。若您未滿二十歲，應於您的法定代理人閱讀、瞭解並同意本同意書之所有內容及其後修改變更規定後，方得使用本服務，但若您已接受本服務，視為您已取得法定代理人之同意，並遵守以下所有規範。

一、基本資料之蒐集、更新及保管

(一)本校蒐集您的個人資料在中華民國「個人資料保護法」與相關法令之規範下，依據本校「隱私權政策聲明」，蒐集、處理及利用您的個人資料。
(二)請於申請時提供您本人正確、最新及完整的個人資料。
(三)本校因執行業務所蒐集您的個人資料包括姓名、職稱、聯絡方式(E-Mail、電話及地址)等(視實際狀況，各表單自行調整)。
(四)若您的個人資料有任何異動，請主動向本校申請更正，使其保持正確、最新及完整。
(五)若您提供錯誤、不實、過時或不完整或具誤導性的資料，您將損失相關權益。
(六)您可依中華民國「個人資料保護法」，就您的個人資料行使以下權利：
1、請求查詢或閱覽。2、製給複製本。3、請求補充或更正。4、請求停止蒐集、處理及利用。5、請求刪除。

但因本校執行職務或業務所必須者，本校得拒絕之。若您欲執行上述權利時，請參考本校「隱私權政策聲明」之個人資料保護聯絡窗口聯絡方式與本校連繫。但因您行使上述權利，而導致權益受損時，本校將不負相關賠償責任。

二、蒐集個人資料之目的

(一)本校為執行gm2電子郵件帳號申請業務(視實際狀況，各表單自行調整)需蒐集您的個人資料。
(二)當您的個人資料使用方式與當初本校蒐集的目的不同時，我們會在使用前先徵求您的書面同意，您可以拒絕向本校提供個人資料，但您可能因此喪失您的權益。
(三)本校利用您的個人資料期間為即日起至您於本校畢業後3年內(視實際狀況，各表單自行調整)，利用地區為台灣地區。

三、基本資料之保密

本校如因天災、事變或其他不可抗力所致者，致您的個人資料被竊取、洩漏、竄改、遭其他侵害者，本校將於查明後以電話、信函、電子郵件或網站公告等方法，擇適當方式通知您。

四、同意書之效力

(一)當您勾選「我同意」並簽署本同意書時，即表示您已閱讀、瞭解並同意本同意書之所有內容，您如違反各該條款時，本校得隨時終止對您所提供之所有權益或服務。
(二)本校保留隨時修改本同意書規範之權利，本校將於修改規範時，於本校網頁(站)公告修改之事實，不另作個別通知。如果您不同意修改的內容，請勿繼續接受本服務。否則將視為您已同意並接受本同意書該等增訂或修改內容之拘束。
(三)您自本同意書取得的任何建議或資訊，無論是書面或口頭形式，除非本同意書條款有明確規定，均不構成本同意條款以外之任何保證。

五、準據法與管轄法院

本同意書之解釋與適用，以及本同意書有關之爭議，均應依照中華民國法律予以處理，並以臺灣臺南地方法院為管轄法院。

□我已閱讀並接受上述同意書內容　當事人簽名：_____中華民國__年__月__日

個人資料處理及利用之基本管控重點

- Data minimization（ISO29100, 5.5）
  - 只蒐集與處理最小做用個資需求
  - 確保個資之最小揭露需求
  - 符合內部工作職權之個資接觸
  - 確保個資關聯的最小使用
  - 符合最小個資保存與銷燬

資料極小化

- Use, retention and disclosure limitation（ISO29100, 5.6）
  - 限制個資使用、保存與公開傳輸，以確保符合個資保護要求
  - 確保個資使用符合特定目的之規範
  - 確保個資保存之最小需求
  - 落實個資銷毀或去名化之安全作業
  - 當個資使用目的結束時，若因法律或相關規範需求而進行個資檔案保存時，該個資應予以封鎖
  - 若個資有進行國際或跨境傳輸時，組織應確保個資傳輸之安全保護

利用、持有與揭露限制

個人資料儲存及銷毀管控重點

- 儲存應注意保存年限，不必要的複本盡量降低產生之數量與份數。
- 紙本資料儲存應注意環境與安全問題，例如：溫濕度、消防設備、門禁管制等；電子資料儲存應注意設備安全與存取控制問題，例如：設備資安漏洞更新、資料存取權限、加密儲存、上櫃上鎖、進出紀錄等。
- 超過保存年限或業務不需要再使用之個人資料應規劃銷毀或刪除作業。
- 紙本資料可造冊確認銷毀之數量及範圍，並留存相關銷毀紀錄，例如：拍照、錄影、銷毀人員及監銷人員確認；電子資料應留存儲存媒體銷毀紀錄、電子檔案刪除過程與結果截圖。

個人資料紀錄銷毀申請單

文件編號：NUTN-PIMS-D019 紀錄編號：	版次：1.0 申請日期：　年　月　日	機密等級：限閱

本表單蒐集之個人資料，僅限於特定目的使用，非經當事人同意，絕不轉做其他用途，亦不會公佈任何資訊，並遵循本校資料保存與安全控管辦理。

申請單位	
申請人員	
個資檔案清冊名稱	
銷毀資訊	□起迄流水號_____~_____ □起迄日期____年____月____日~____年____月____日 □數量_____
銷毀方式	□自行銷毀　□委外銷毀
委外銷毀陪同人員	（委外銷毀始需填寫此欄位）
委外銷毀廠商	（委外銷毀始需填寫此欄位）
銷毀日期	____年____月____日

承辦人	委外銷毀陪同人員	單位主管	文管人員
	（委外銷毀始需填寫此欄位）		

註 1：若委外執行銷毀，應確認相關陪同紀錄已附於此表單，始得存檔。
註 2：本表單之保存期限為至少保留三年。

個資生命週期之安全管理

蒐集

蒐集的理由、適法與利用目的告知義務
只要有蒐集的行為，就會有告知的義務

傳輸

傳輸過程中之安全
-電子檔案傳輸應加密
-紙本檔案應彌封或專人傳送

儲存

-存放個人資料場所及設備之安全管理
-備份或歸檔後之資料安全
-個資檔案清冊

利用

符合個人資料保護法§16之使用規範與蒐集之特定目的相符或特定目的外之利用

銷毀

個資刪除或報廢之安全處理程序
-紙本檔案碎紙機、水銷
-資料抹除、硬碟銷毀

tsc 遠東 TSC CAPITAL GROUP
The Bridge to the Asia Pacific Region

網路存取與使用設備安全管理

- 不隨意下載免費或不明軟體（破解版）
- 不隨意開啟電子郵件之連結與附件
- 傳遞敏感之資料應以安全方式進行
  -資料加密後傳遞
  -傳送後立即與對方確認
- 含有敏感訊息之廢紙應立即銷毀
- 盡量不蒐集過多之個資
- 密碼應妥善保管並定期更改
- 電腦作業系統及使用軟體應定期更新
- 離開電腦座位時應使用電腦鎖定功能。

快捷鍵:〔視窗鍵〕+〔L〕

25款惡意程式下載數破數百萬！FB帳戶被看光…Google Play悄悄下架

匯流新聞網 | 2.3k 人追蹤 追蹤

林 欣穎
2020年7月2日 下午5:51

2 則留言

匯流新聞網記者林欣穎／台北報導

現代人人手一機早已成為常態，各式各樣的應用服務與科技結合，讓民眾可以透過手機滿足生活所需與娛樂，不過也有不少有心人士看中這點，在這些實用的免費軟體中埋藏惡意程式軟體，悄悄竊取你手機中的重要訊息！近期根據外媒報導，Google從應用程式商店中悄悄下架了25款惡意應用程式，原來這些程式都在偷取你的資料。

Google Play是Google旗下、安卓系統使用的的應用程式商店，裏頭的程式功能包羅萬象，不管是影視服務、遊戲、實用小功能、社群平台還是拍照程式應有盡有，不過先前早有資安機構指出，Google Play上有不少來源不明、藏有木馬病毒的程式，隱藏在免費軟體中，誘使民眾下載。

tsc 德飛 TSC CAPITAL GROUP The Bridge to the Asia Pacific Region

釣魚網站騙取個人資料-加油卷免費送範例

https://www.lineoutlet.org/

雙十國慶 加油券免費送

歡慶雙十 加油券免費送!!! 市值500元 失血大放送 僅此一次 ...

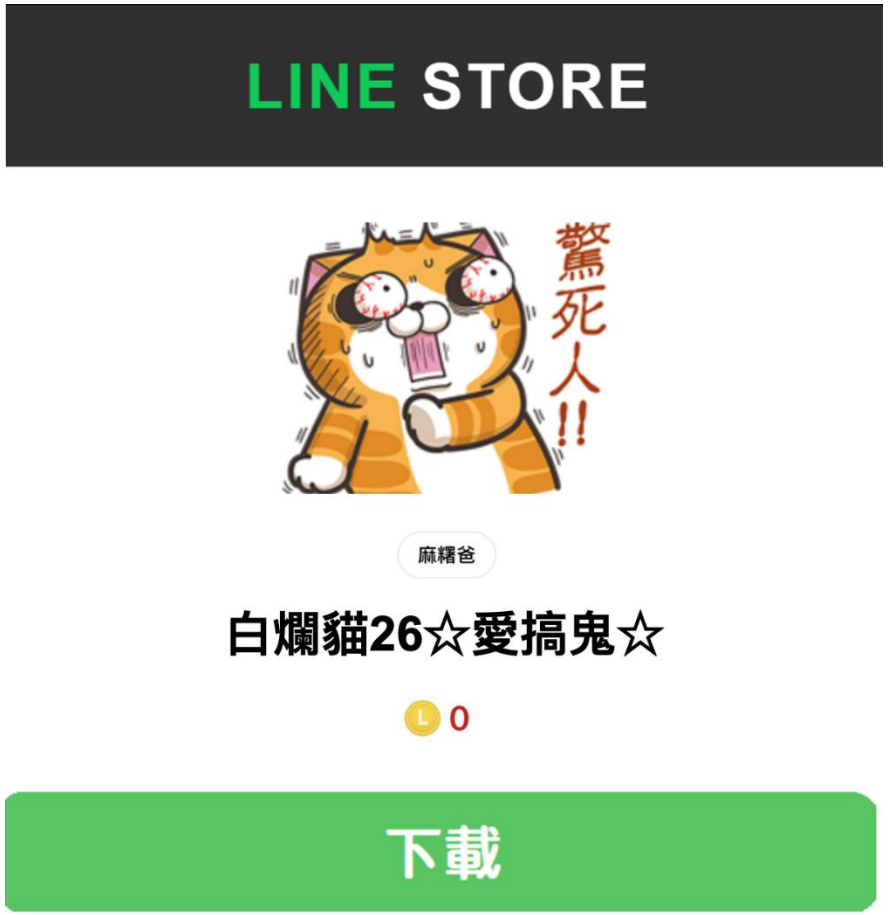
tsc 淡水 TSC CAPITAL GROUP The Bridge to the Asia Pacific Region

釣魚網站騙取個人資料-包裹訊息詐騙範例

個資騙取成功！

tsc 海邦 TSC CAPITAL GROUP The Bridge to the Asia Pacific Region

釣魚網站騙取個人資料-免費Line貼圖範例



密碼安全管理

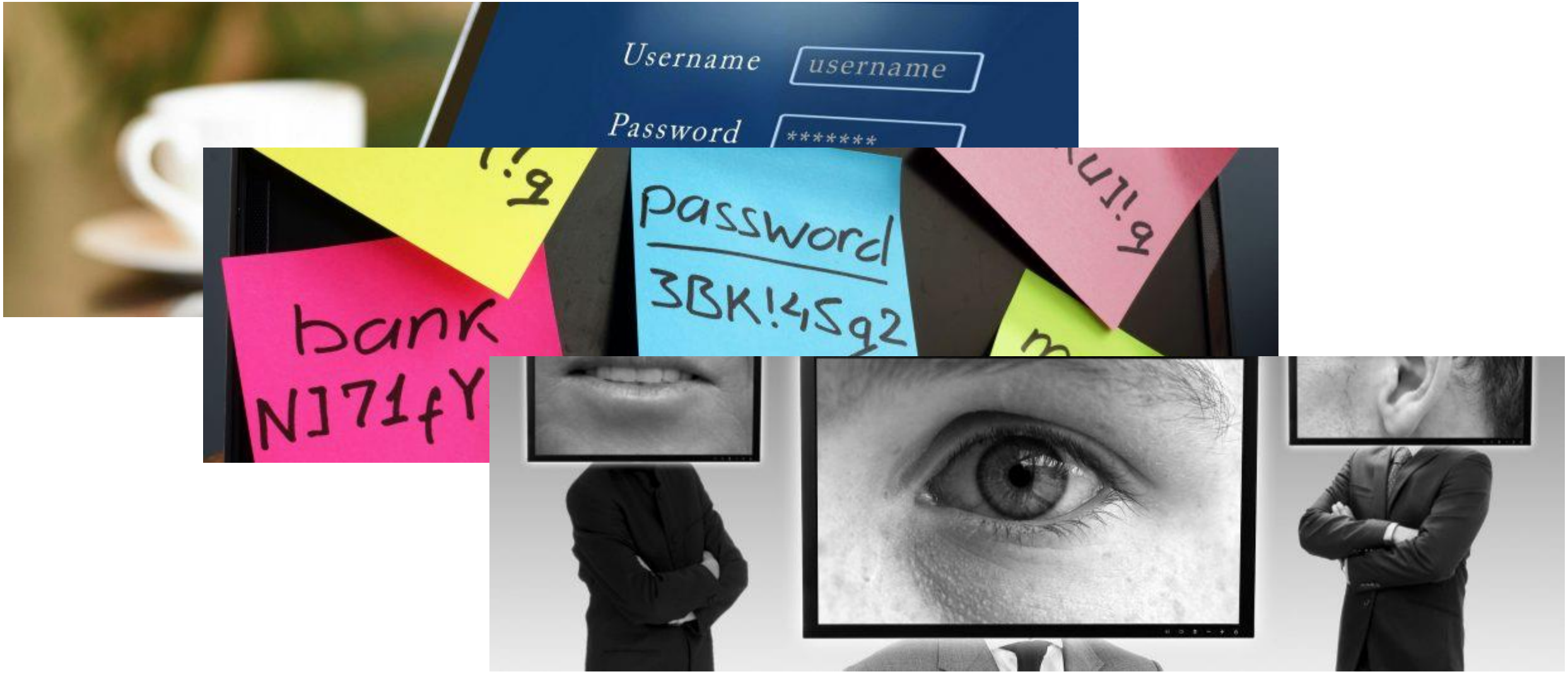
- 若使用服務有預設密碼，應立即更改。
- 密碼長度至少8碼以上，並符合密碼複雜度原則(特殊符號/英文大小寫/數字)。
- 定期更換密碼。
- 避免多個系統使用同組密碼，以免遭受撞庫攻擊。
- 善用雙因子/多因子認證(Two-Factor/Multi-Factor Authentication，2FA/MFA）或動態密碼（One-Time Passwords，OTP）
- 勿將密碼書寫於明顯且容易讓他人取得之處。

請記住，雙因子身份驗證通常不會預設啟用，因此您必須為每個重要的帳戶(例如銀行、投資、退休 或個人電子郵件)自行啟用。雖然一開始似乎需要更多的手續，但一旦設定好就非常容易使用。

電子資料加解密防護

- 電子檔案加解密可應用於電子檔案儲存或傳送，以保護資料之機密性、完整性。
- 常用軟體Microsoft Office、 Adobe Acrobat 、LibreOffice、7-zip、均具有檔案加密之功能，建議傳輸電子檔案時使用加密功能。

個人資料保護議題



何謂社交工程？

- 社交工程兩個基本要件：
  - 第一個是【人】
  - 第二個是【詐騙手法】
- 凡對【人】甚至於【特定對象】，使用各種【詐騙手法】，獲得不當資訊，來達到施騙者的目的，都可稱之為【社交工程】。

重要人事異動公告	接到電話說自己小孩被綁架了。
網路購物商場人員誤選分期付款。	某某明星爆出私生子新聞。
長官要求提供業務機敏資訊。	帳戶異常請登入此網站做處理。

tsc 海外 TSC CAPITAL GROUP The Bridge to the Asia Pacific Region

電子郵件社交工程安全防護須知

收到來路不明信件你會怎麼做？

- 確認寄件來源及寄件者
- 確認信檢主旨及郵件內容
- 判斷是否跟業務有相關
- 審慎查證寄件人(ex.電話)

tsc 淘帝 TSC CAPITAL GROUP The Bridge to the Asia Pacific Region

國立臺南大學111年電子郵件社交工程演練結果說明(1/3)

- 執行期間：111年6 月11日至111年7月8日
- 受測總人數：全校504位同仁
- 發信總數：2,520封

項次	類型	演練郵件主旨
1	保健類	濕熱體質易好發汗皰疹 烤、炸、辣、酒不要碰
2	科技類	越來越多人不相信食評網評價 Google地圖將會一統天下？
3	個人訊息類1	人壽保險費委託轉帳/信用卡通知書(請輸入身分證號碼開啟附件)
4	個人訊息類2	PChorne線土購物-構買清單(訂單編號：202306119016111)
5	個人訊息類3	土地銀行【非約定轉帳結果通知】

國立臺南大學111年電子郵件社交工程演練結果說明(2/3)

- 本次演練成功觸發結果

檢測項目	測試人數	總信件數	觸發人數	比率
開啓信件人數(比率)	504	2520	36	7%
點擊連結人數(比率)			64	13%
開啓附件人數(比率)			65	13%

公務郵件信箱之使用，應避免使用個人信箱收發公務郵件，或使用公務郵件處理私人用途，對於各信件主旨，來源寄件者名稱、內容判斷等，應持續保持「停」、「看」、「聽」原則～

社交工程信件範例

國立臺南大學111年電子郵件社交工程演練結果說明(3/3)

- 各類型信件觸發動作數量統計

項次	類型	演練郵件主旨	觸發動作	觸發動作數量
1	保健類	濕熱體質易好發汗皰疹 烤、炸、辣、酒不要碰	開啓信件	4
			點擊連結	3
			開啓附件	1
2	科技類	越來越多人不相信食評網評價 Google地圖將會一統天下？	開啓信件	6
			點擊連結	1
			開啓附件	1
3	個人訊息類1	人壽保險費委託轉帳/信用卡通知書(請輸入身分證號碼開啟附件)	開啓信件	24
			點擊連結	23
			開啓附件	27
4	個人訊息類2	PChorne線土購物-構買清單(訂單編號：20230611901611)	開啓信件	12
			點擊連結	13
			開啓附件	15
5	個人訊息類3	土地銀行【非約定轉帳結果通知】	開啓信件	18
			點擊連結	31
			開啓附件	33

LINE真假訊息求證防詐騙及陌生來電識別

LINE官方帳號搜尋:
趨勢科技防詐達人

LINE 訊息查證官方帳號：
@linefactchecker

Whoscall 來電號碼辨識APP

警政署為增強防制力道，協助辨識來電者真實身份，從2016年6月份起，與Whoscall公司合作，透過政府165反詐騙專線的大數據整合，目前民眾利用Whoscall APP可協助辨識超過6000萬筆電話號碼，大幅阻擋詐騙、推銷、騷擾等惡意電話。

案例分享與討論

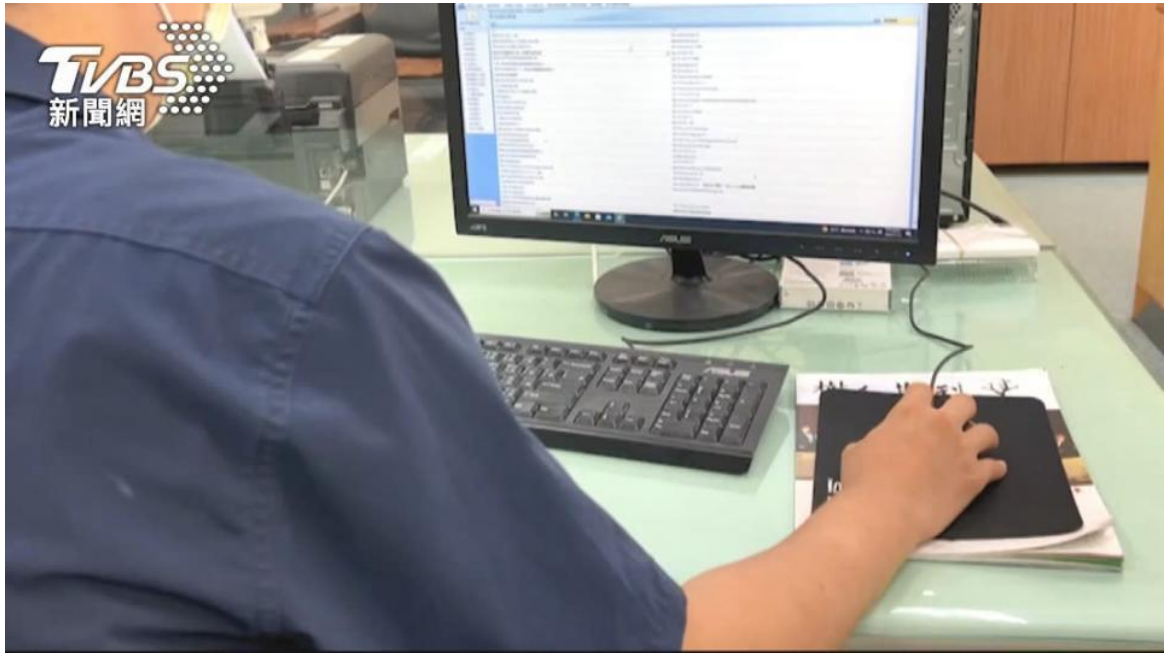
案例1.上班用公務電腦查啦啦隊個資 員警下場GG所長連帶處分

台南市一名員警，利用警政電腦系統，偷偷查詢職棒啦啦隊成員的資料，由於內部有人看不下去，在臉書社群爆料，質疑有人包庇，分局立刻發表聲明，強調依法處理，該名員警火速被記過、停權，連所長都遭到連帶處分。

南市第四警分局督察組長郭榮木：「調查後是基於該員個人好奇心，未涉及洩密，已針對該員加重核宜，記過兩次處分，並暫停該員查詢權限。」

被點名的是台南市警局，四分局華平所的一名劉姓員警，他涉嫌在六月份，利用上班時間，偷查啦啦隊成員資料，雖然消息曝光，分局強調連所長都被連帶處分，但看在律師眼裡，恐怕涉及的還有法律層面。

原來根據法規，警務人員要查詢當事人個資，除了要有法律的明文規定，還有當時正在執行法定職務，或是有公益目的，否則就要當事人願意公開以及有學術目的，但顯然這名員警，利用上班時間查詢，只為了滿足個人私利而且還連帶讓其他員警，使用個資查詢系統的威信受到質疑。



#使用目的　#軌跡資料　#證據保存

資料來源：https://tw.news.yahoo.com/上班用公務電腦查啦啦隊個資-員警下場gg所長連帶處分-153053435.html

案例3.日本外包業者弄丟46萬個資隨身碟

日本兵庫縣尼崎市發生市府外包業者遺失存有46萬名市民個資等資料的USB隨身碟事件，雖然最後順利找回且資料看似未外流，但幾天來逾萬市民致電市府表達不滿等，網友也罵翻。

日本富士新聞網報導，尼崎市長稻村和美6月24日傍晚在記者會上說，裝有USB隨身碟的包包已被尋獲，造成全體市民感到困擾及擔心，「由衷致上歉意」。

這起隨身碟遺失事件發生在6月21日，當天外包公司配合廠商的一名40多歲男員工，帶著這顆存有尼崎市所有市民個資、稅務資料及受領生活補助金等資料的隨身碟外出，並在餐飲店喝完酒後遺失自己所攜帶的包包。

外包公司表示，男子並未在第一時間回報公司，而是請了一天假自己去找包包，但因為遍尋不著，最後向警方求助。

為避免隨身碟內資料外洩，警方罕見動員了約30人協助尋找遺失物，最後在大阪府吹田市內一處大樓入口處尋獲。由於包包內有行動電話，研判行動電話位置資訊在尋找過程中發揮作用。

#委商管理 #資料管理 #事件管理

資料來源：https://udn.com/news/story/6812/6415288

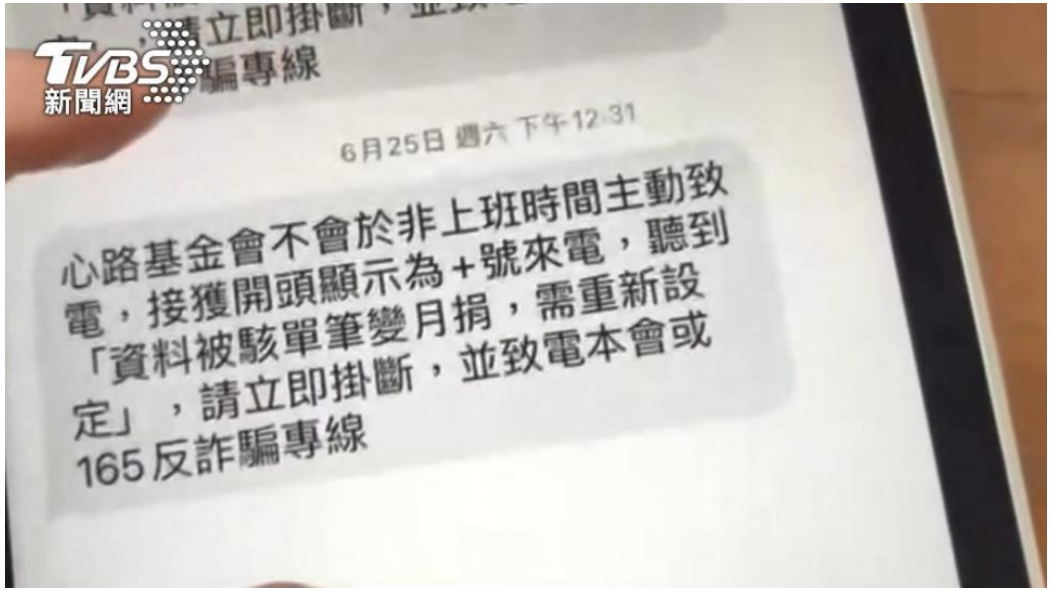
案例2.捐款人個資遭駭！「假公益詐騙」單月逾5百萬

捐款給公益團體的善心，卻被不肖人士變成斂財工具，有民眾長期捐款心路基金會，最近卻不斷收到基金會傳來簡訊要他小心遭騙，一問之下才知道原來基金會捐款人的個資遭到駭客入侵，一個月內就有300位捐款人街道詐騙電話，甚至有10多位已經被騙錢，原來早在去年就已經有超過60家公益團體也遭駭入，光今年3月受詐騙的總金額就超過5百萬元。

心路基金會表示，有不少捐款人接到詐騙電話，謊稱工作人員操作錯誤，定期定額捐款有問題，要到ATM操作或是用網銀匯出款項，基金會捐款人資訊，從6月開始就被駭客入侵，光是1個月內就有超過300通的諮詢，且有10多位捐款人已經被騙錢。

今年1到5月因為疫情，捐款比同期少800萬，6月捐款人個資遭駭後大受影響，比往年同期少200萬，運來被駭入的公益團體不只心路基金會，去年有逾60家大多使用相同維護系統因此同事被駭入，今年1到6月也有7、8家，使用不同維護系統的公益團體捐款人資料遭竊取。

公益團體紛紛貼出公告要捐款人小心受騙，經警政署165專線統計光今年3月受理假冒「公益團體」詐騙報案就有24件，總財損金額超過500萬元，平均每位民眾被騙數萬到數十萬。



#個資事件 #社交工程 #組織聲譽

資料來源： https://tw.news.yahoo.com/捐款人個資遭駭-假公益詐騙-單月逾5百萬-145232466.html

案例5.財政部國稅局爆發記帳士個資外洩 行政院列資安事件

財政部國稅局傳出資安事件。財政部中區國稅局一名承辦人在建置記帳士查詢名冊時，疑人為疏失，誤將記帳士個資檔案傳輸上網，導致身分證字號、地址、出身年月等個資全都露，目前有國外網站將這些記帳士資料備份庫存，法界人士憂心，若資料被駭客拿去「暗網」兜售，後果相當嚴重，行政院目前將此事列為資安事件處裡。

備份財政部中區國稅局資料的網站是「台灣公開資訊網」，此網站在美國註冊，設立目的想讓民眾方便搜尋政府公開資料，但沒想到卻發生誤將記帳士個資上傳一事，目前中區國稅局已緊急將資料更新下架，但「台灣公開資訊網」庫存頁面依然存在，且該網站無聯絡人，想要對方下架恐非易事，除中區國稅局外，其他分區並無此情況發生。

目前該服務已無法讀取，但DNS cache尚存在。

資料來源：https://udn.com/news/story/7314/5927958

#人員管理 #資料管理 #事件管理

tsc 遠東 TSC CAPITAL GROUP The Bridge to the Asia Pacific Region

課程總結

課程總結

- 業務執行時所使用之個資資料，應遵守最小化原則。
- 個資處理或利用應不逾越蒐集個資之特定目的。
- 傳遞個資資料應以安全方式進行，個資資料處理與銷毀應更加謹慎。
- 密碼應有複雜度設置及定期更換習慣，並建議開啟雙/多因子驗證設定。
- 駭客攻擊與非法人士詐騙手法與日俱進，應隨保持資安與個資保護緊覺性。
- 資訊安全是持續精進的風險管理，資訊安全亦包含個人資料安全管理。

當面對駭客攻擊時，您自己就是最佳的資安防禦，善用常識，保持警覺！

TSC CAPITAL GROUP
The Bridge to the Asia Pacific Region

問題與討論

請掃描QR code填寫課後評量

https://forms.gle/CA23KrEQvdNsC1Gp9

TSC CAPITAL GROUP

The Bridge to the Asia Pacific Region

感謝您的參與

歡迎於活動後與講師討論您的任何疑問

本公司的臉書粉絲團及部落格可以找到更多資訊

TSC – FB Site

TSC – Blog Site