國立臺南大學

資通安全暨個資保護認知宣導教育訓練

講者：漢昕科技管理顧問 劉書瑜

日期：115年6月16日

本次教育訓練目的


資通安全素養
ODF開放文件應用
資訊資產盤點
資安政策宣導
個資保護與智財認知
個資管理政策宣導
個資盤點與風險評驗
個人資料管理

AGENDA

1. 近期資安威脅概述
2. 常見的網路攻擊態樣
3. 社交工程攻擊與防範
4. 保護智慧財產權、ODF開放文件應用、資通安全政策宣導

BCCS 漢昕科技
-能你最近的資安專家-

2025年最常被國家級駭客鎖定的國家

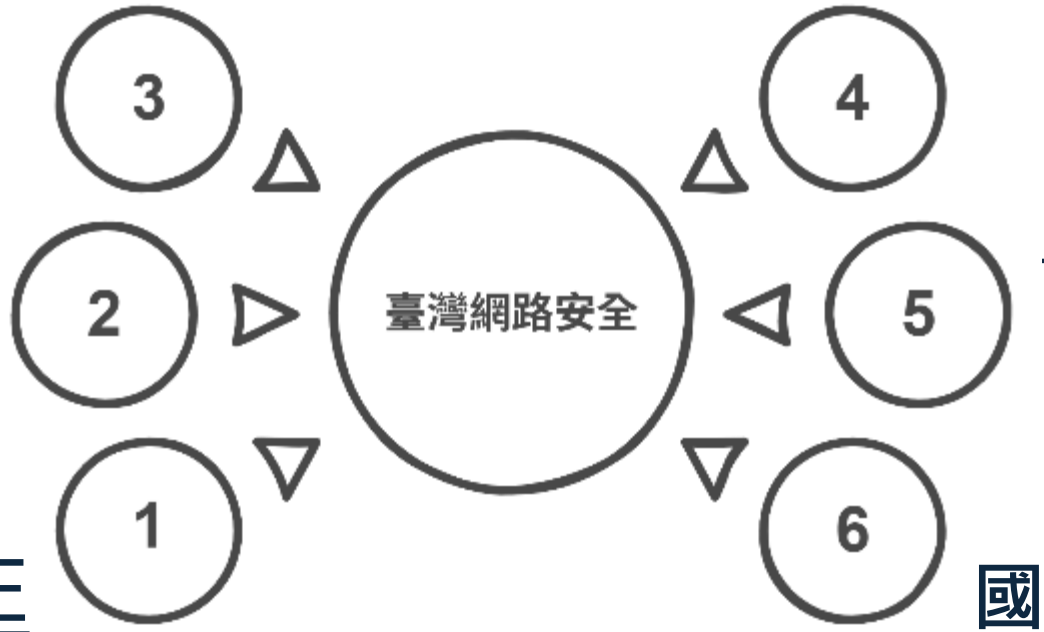
2025 年 Microsoft 數位防禦報告

過去一年的資通訊安全概況

酷澎個資外洩
中國籍前員工所為，洩露3,370萬名用戶的個資

AI Agent風險浮現
與AI助理的對話被蒐集、瀏覽器中任何AI助理都有風險

ClickFix/FileFix攻擊
此類手法日益猖獗



駭客組織互相合作
ShinyHunter與Scattered Spider共同鎖定受害者並分享攻擊工具與手法

法規制定與修正
資通安全管理法及其相關子法、人工智慧標準法、個人資料保護法(尚未施行)

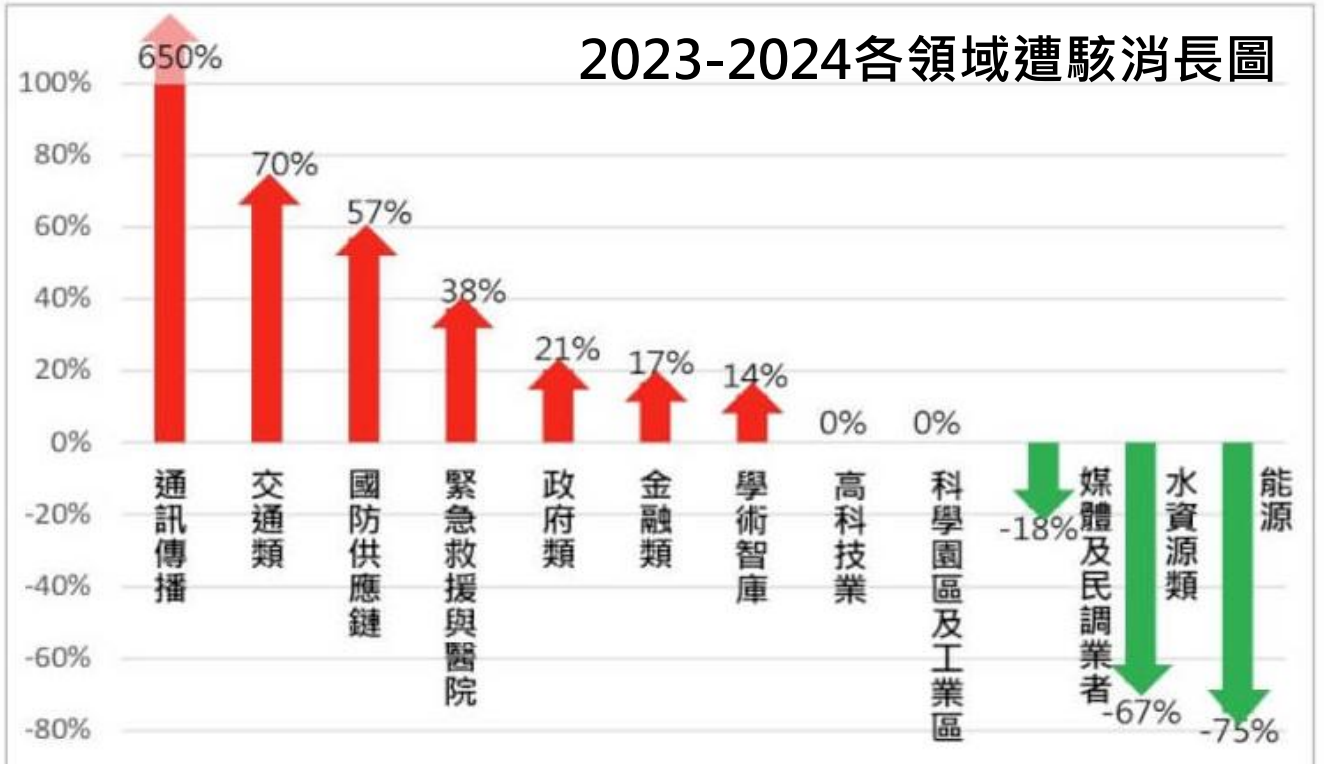
國家級駭客攻擊
聯合安全公報警告中國駭客已經滲透全球的關鍵基礎設施，尤其是電信服務業

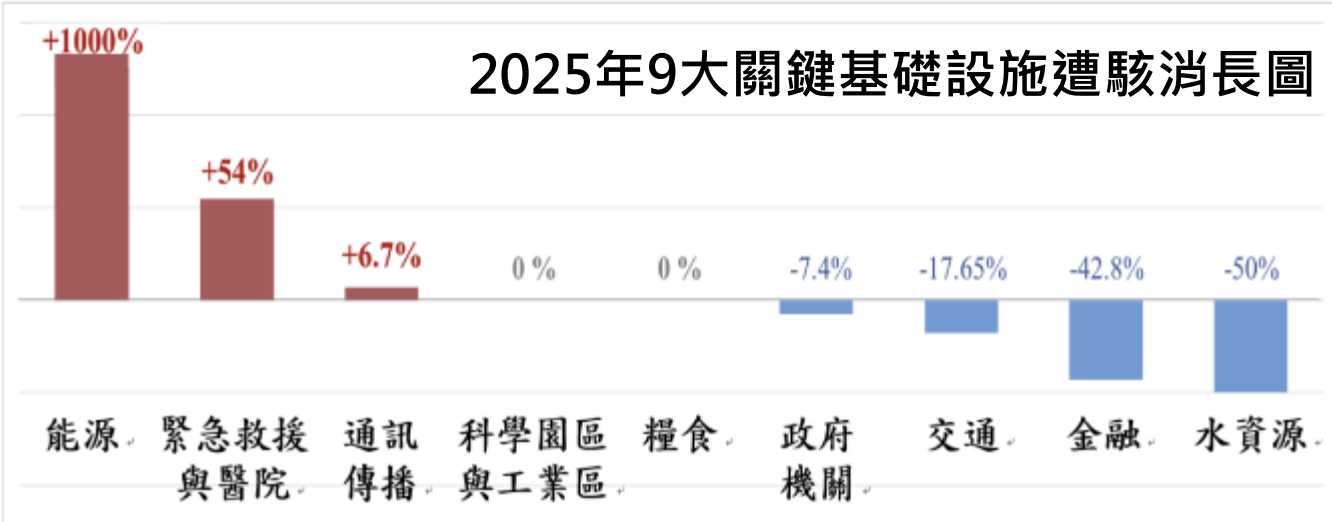
過去一年針對關鍵基礎設施的主要攻擊

國安局發布「2025年中共對我國關鍵基礎設施網駭威脅分析」報告

以「DDoS 分散式阻斷服務攻擊」、「軟硬體漏洞攻擊」、「社交工程攻擊」及「供應鏈攻擊」等方式，侵擾數平均每日約達263萬次

波蘭國鐵緊急剎車訊號網路攻擊事件





AGENDA

1 近期資安威脅概述

2 常見的網路攻擊態樣

3 社交工程攻擊與防範

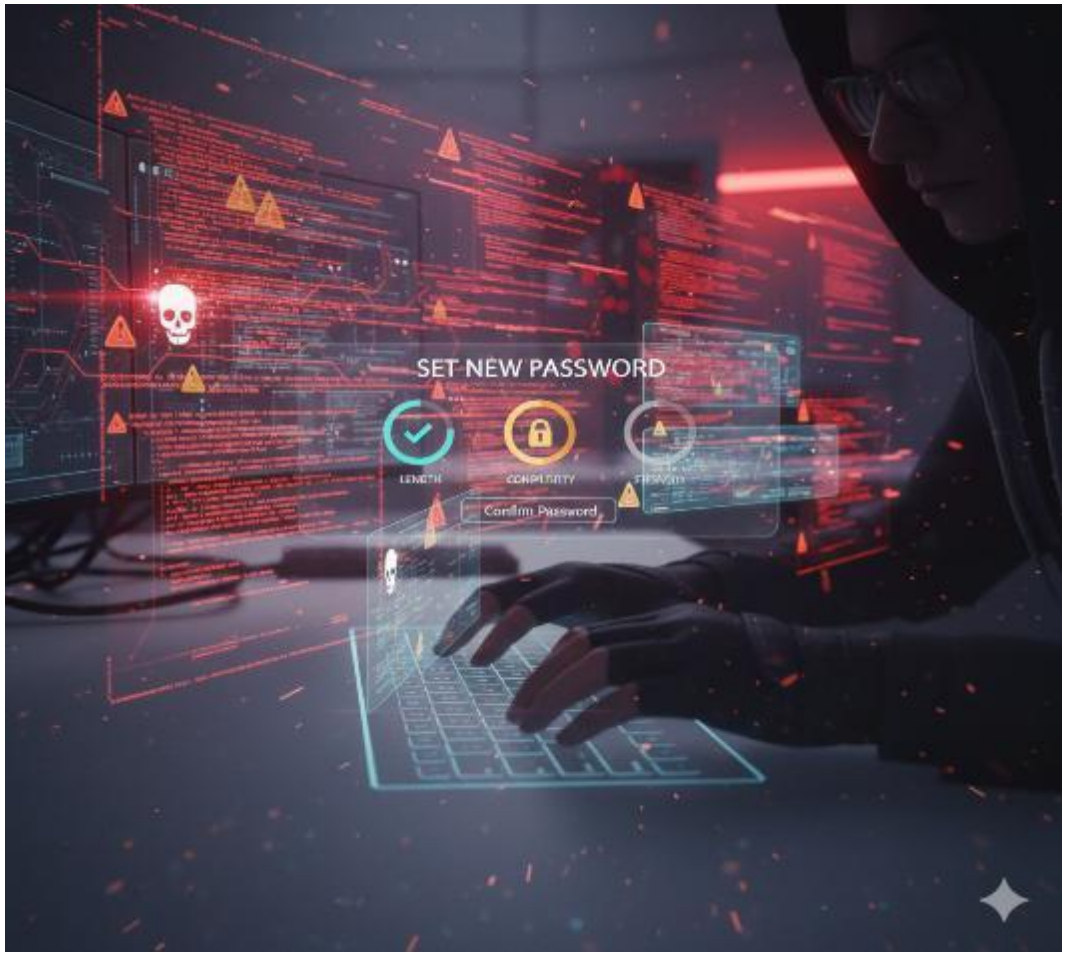
4 保護智慧財產權、ODF開放文件應用、資通安全政策宣導

BCCS 漢昕科技
-能你最近的資安專家-

什麼是網路攻擊?

- 指個人或組織基於惡意故意嘗試入侵其他個人或組織的資訊系統，攻擊者通常會藉由中斷受害者的網路尋求某些利益。

- 目標在於對企業或個人電腦造成損害、取得控制權或存取重要的文件、資料。



為什麼我們要保護資訊？資安三要素 (CIA)

- 機密性 (Confidentiality)： 只有「對的人」能看到特定的資料。
- 完整性 (Integrity)： 確保資訊資產「沒被偷偷被改過」。
- 可用性 (Availability)： 想用資訊資產時「隨時能用」。

網路攻擊態樣


搜尋圖片商品
訂單程票
訂去回票
實名制訂票
查詢/取消訂票
訂便當作業
團體訂票
優惠特區
Home / Order train tickets / Random numbers check
圖片驗證檢查
請輸入圖形中的英數字:
7Z851
語音播放
重新產生驗證碼
傳送中...
網路訂票系統暫停服務
統維護作業，目前無法提供服務，請稍後再試。
naintenance, THSRC corporate website is sus
SETN三立新聞網
南港
左營
交易失敗!
購票系統忙碌中，請稍後重新操作。
確定

網路攻擊態樣

暴力攻擊

- 暴力破解帳號密碼，利用使用反覆試驗來嘗試猜測密碼

撞庫攻擊

- 利用外洩的帳戶密碼，於不同平台嘗試登入、盜用帳號

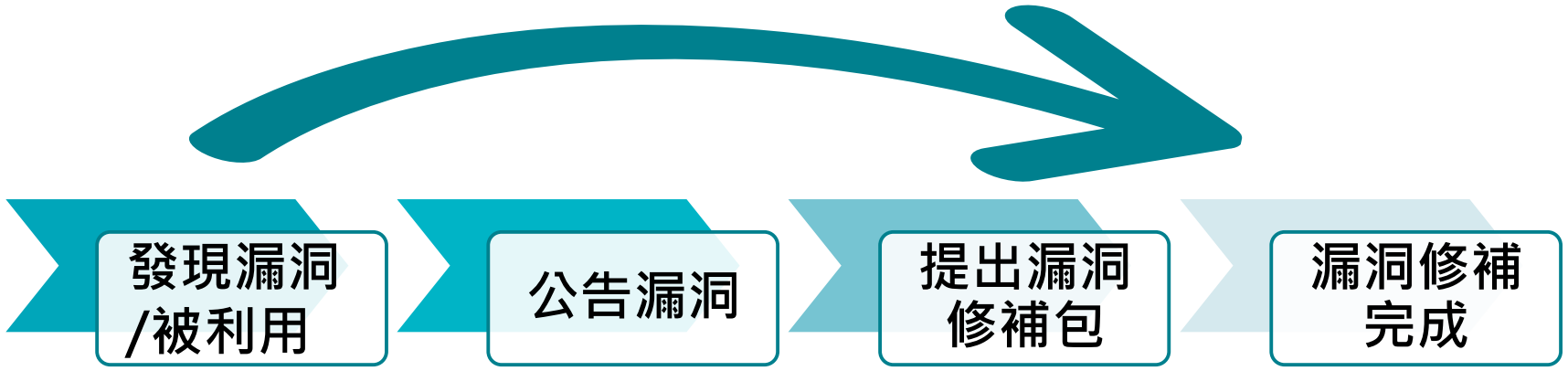
```
[80][http-get-form] host: 192.168.100.155   login: admin   password: password
[80][http-get-form] host: 192.168.100.155   login: admin   password: p@ssword
[80][http-get-form] host: 192.168.100.155   login: admin   password: 12345
[80][http-get-form] host: 192.168.100.155   login: admin   password: 1234567890
[80][http-get-form] host: 192.168.100.155   login: admin   password: Password
[80][http-get-form] host: 192.168.100.155   login: admin   password: 123456
[80][http-get-form] host: 192.168.100.155   login: admin   password: 1234567
[80][http-get-form] host: 192.168.100.155   login: admin   password: 12345678
[80][http-get-form] host: 192.168.100.155   login: admin   password: 1q2w3e4r
[80][http-get-form] host: 192.168.100.155   login: admin   password: 123
[80][http-get-form] host: 192.168.100.155   login: admin   password: 1
[80][http-get-form] host: 192.168.100.155   login: admin   password: 12
1 of 1 target successfully completed, 12 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-07-27 15:28:24
```

2025年看似兩間不同的公司發生帳號被盜，將會員點數兌換的事件，後續被證實是撞庫事件

網路攻擊態樣

零時差攻擊

- Zero-day
- 利用尚未修補的安全漏洞進行攻擊。



網路攻擊態樣

進階持續性滲透攻擊(APT)

- 通常是組織型駭客，潛伏時間長，手法細膩
- 即使成功偵測到一次惡意程式，也不代表可以阻止攻擊

偵查

- 收集資訊
- 進行版本探測

對應

- 確認網路架構
- 尋找web應用程式的資源存放位置

發現

- 透過軟體/系統版本，找到攻擊進入點

利用

- 利用弱點發出攻擊
- 繼續潛伏等待時機

網路攻擊態樣

進階供應鏈攻擊(Supply Chain Attack)

- 利用受信任的方式分發惡意程式
- 攻擊可以一次性的影響相當大的範圍
- 規避掉許多傳統的安全防護措施

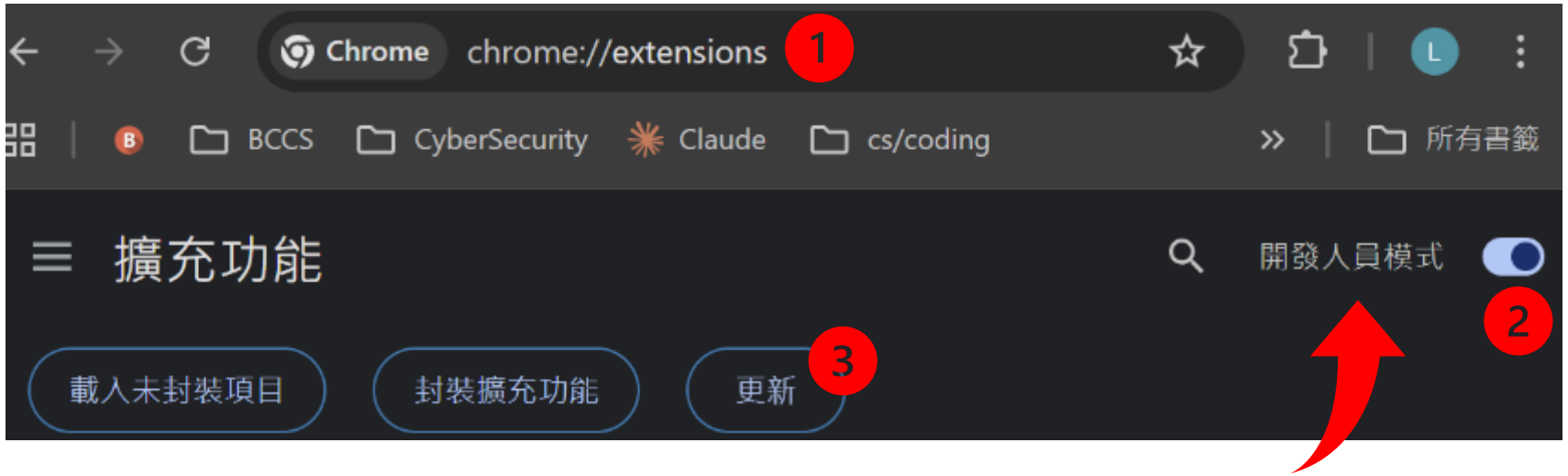
2019年ASUS ShadowHammer事件

https://cdn.prod.website-files.com/635e632477408d12d1811a64/63fc9bab9db293edca4a4f53_word-image-21792-1.png

網路攻擊態樣

擴充元件/套件的惡意威脅

- 利用合法之擴充功能，於後續更新中植入惡意程式碼
- 在 VS Code 延伸套件市集 或 Chrome 線上商店上架名稱與熱門套件極為相似的仿冒品



開發人員模式開啟後，會出現更新按鈕

Chrome 擴充功能更新生命週期

網路攻擊態樣

社交工程

- 利用人性的特點，透過操縱人的心理博取信任、誘使對方產生預期的行為。例如，透露機敏資訊或允許授權
- 目的：竊取資料、獲得利益、入侵設備、冒用身份等

背景調查
- 鎖定目標對象，收集資訊，選擇攻擊方法

取得信任
- 捏造故事，建立關係，騙取信任

騙取資訊
- 開始發動攻擊、騙取資料

切斷聯繫
- 以自然方式終止與目標的互動，並抹除自己的蹤跡

AGENDA

1 近期資安威脅概述

2 常見的網路攻擊態樣

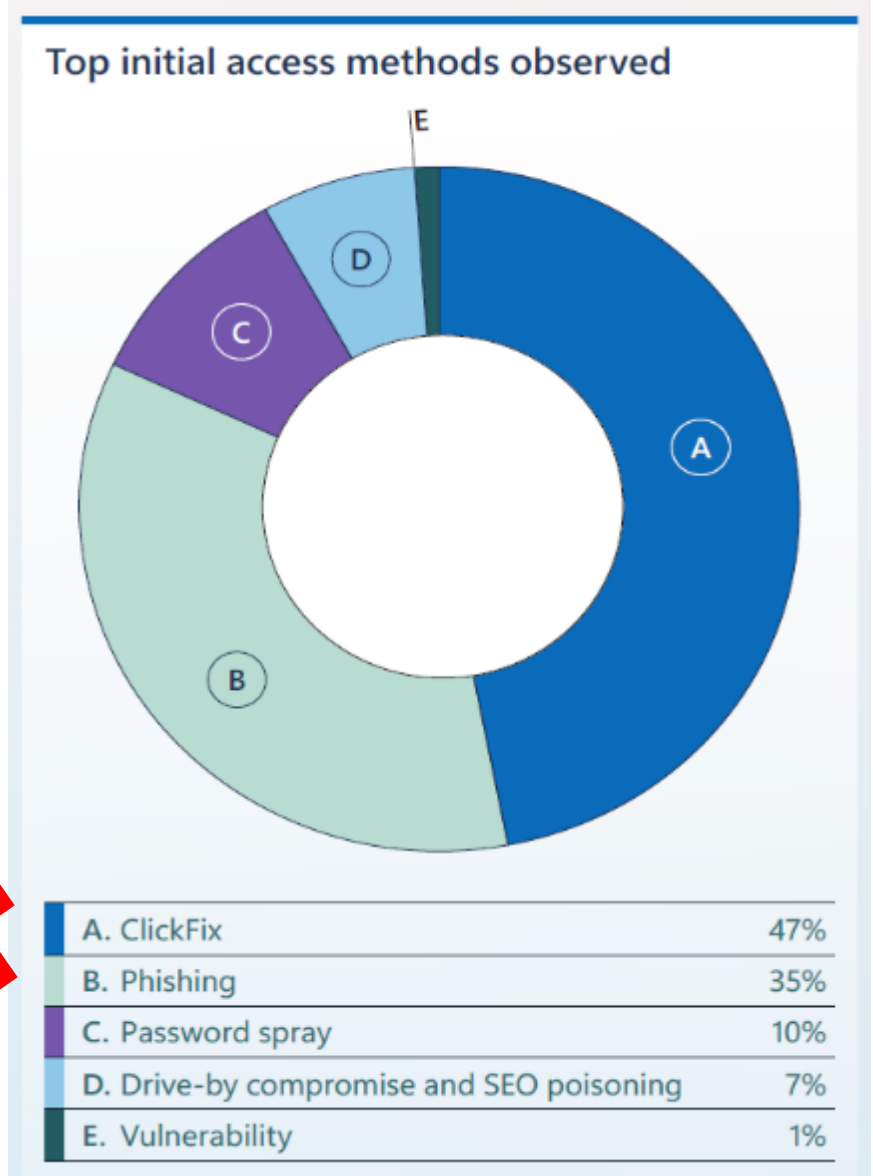
3 社交工程攻擊與防範

4 保護智慧財產權、ODF開放文件應用、資通安全政策宣導

BCCS 漢昕科技
-能你最近的資安專家-

2025年攻擊態樣趨勢

- ClickFix崛起
- 利用漏洞進行攻擊已不再是首選
- 當釣魚威脅越來越普遍，對個人而言，採用多重要素驗證（MFA）能產生顯著效果，因為 MFA 可阻擋超過 99% 的身分識別型攻擊。



2025 年 Microsoft 數位防禦報告

影片連結： https://www.youtube.com/watch?v=XaDeuYIQMOs

社交工程常見手法

尾隨 (Tailgating)

屬於實體面的方法，利用鬆散的出入管制規定，潛入並竊取重要資訊

裝置碼釣魚(Device Code Phishing)

誘使受害者造訪攻擊者設立的網頁，當受害者依要求於手機輸入由攻擊者發送之裝置代碼時，攻擊者同時會取得受害者的微軟服務資訊，進而可以直接存取使用者的微軟服務(M365/outlook等)。

下餌 (Baiting)

提供好處引誘目標對象採取某些行動，例如：贈送可連接電腦的某些小物、免費充電站

充個電手機竟然會中毒？

- 美國FBI特別提醒，盡量避免使用公共空間的免費充電站
- 長期暴露於公共區域的USB插座，很可能已經被動過手腳，能夠在插上充電線時駭入手機，植入惡意軟體。
- 之後回到公司，使用手機與公司電腦系統連線時，間接感染公司設備。

建議：

1. 隨身準備只有充電功能的充電線
2. 找插座而不找USB/type C 孔
3. 充電前將手機/平板傳輸功能關掉

O.MG傳輸線已經存在很久了!!

- 在線頭內藏一顆 Wi-Fi 竊取晶片，透過自行建立一個Wi-Fi熱點來進行運作，在2公里之範圍內有效
- 能透過任何設備打開瀏覽器，竊取遭受攻擊的設備以及紀錄鍵盤輸入的資訊
- $150~$240之間，有各種接頭的版本
- 有心人事也可能會刻意將充電線放在公用充電裝置上，免費提供給其他路人使用

地上的紅包不要撿，免費的Wi-Fi不要連

如何降低風險

- 使用有密碼保護的 Wi-Fi 熱點
- 不要上網購物
- 避免檢查銀行帳戶
- 不要登錄以 http 開頭的網站
- 不要打開藍牙
- Wi-Fi 不要設定成自動連線
- 使用 VPN服務

社交工程常見手法

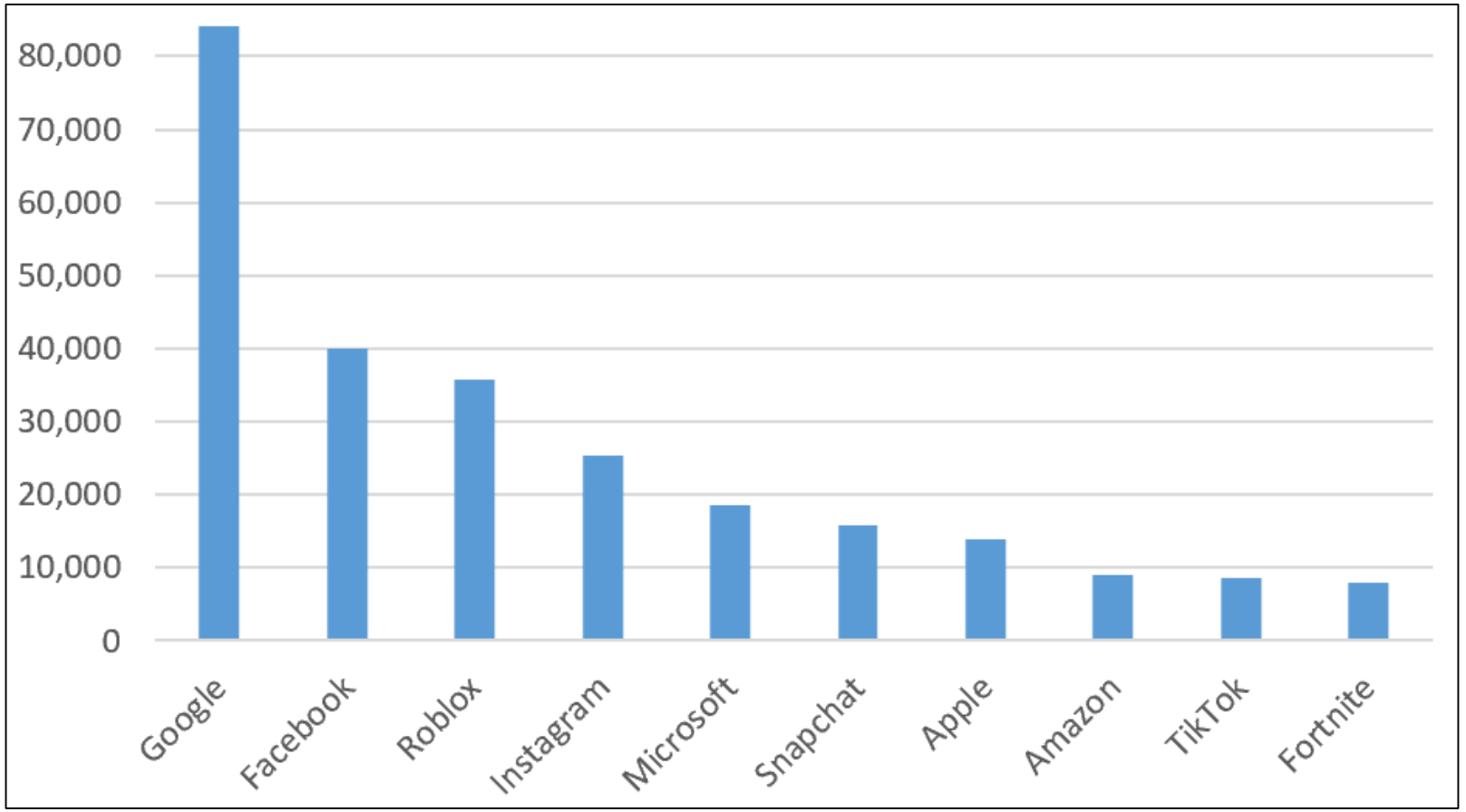
網路釣魚、媒體釣魚

- 是一個總稱
- 媒介種類：網站、媒體、QR code、語音、簡訊、電子郵件
- 佯裝成特定人員，誘騙分享敏感資訊
- 是最常見的社交工程手法

實際案例 – 財政部、遠通ETC

當敵人不再「入侵」而是「登入」

駭客最愛盜Google帳號，國人常用的社群媒體帳號也在排行上



https://www.androidpolice.com/usa-top-exploited-platforms-research/

網站釣魚

網路釣魚網站：偽造中獎網站、抽獎廣告、仿冒成知名網站、時事相關網站

建議：

務必確認網頁名稱是否正確，以及網址是否以https://開頭

社交工程常見手法

搜尋引擎最佳化下毒(SEO下毒)

- 利用SEO(Search Engine Optimization)下毒手法，操控搜尋引擎排名，當使用者搜尋特定關鍵字或網站時，會優先顯示與攻擊目的相關的轉址廣告
- 也會利用Google贊助商廣告
- 建議優先選擇下方有藍勾勾或非廣告的自然搜尋結果

釣魚服務平台(Phishing as a Service/PhaaS)

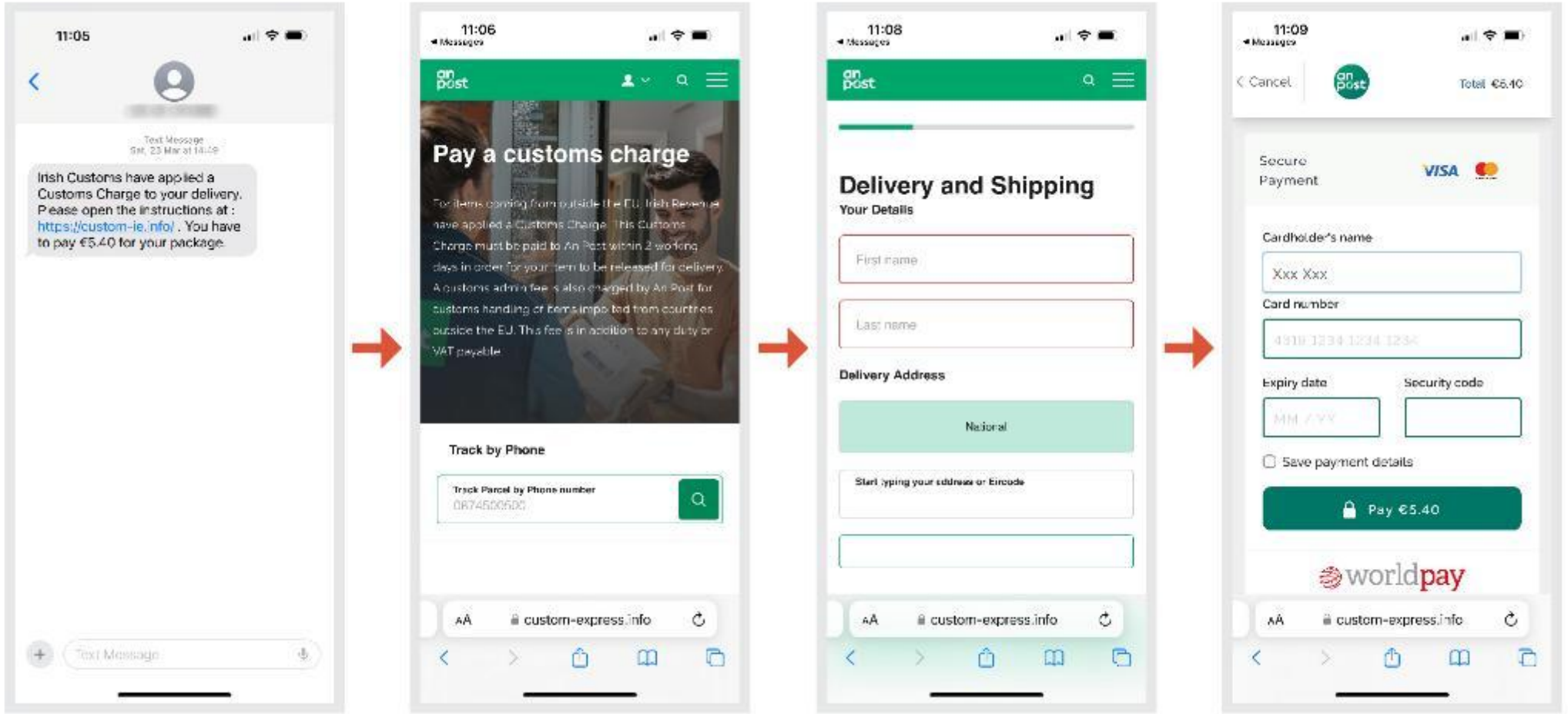
LabHost破獲後，還有Lucid? Lighthouse? 更多?!

- PhaaS將釣魚樣板、發布流程與反監控機制打包成服務，以訂閱或租用方式提供
- 提供沒有專業技術背景的攻擊者快速建立仿冒網站
- 樣板涵蓋金融、政府、郵務與道路收費等產業

高級會員月費 USD 300

https://www.trendmicro.com/zh_tw/research/24/d/labhost-takedown.html

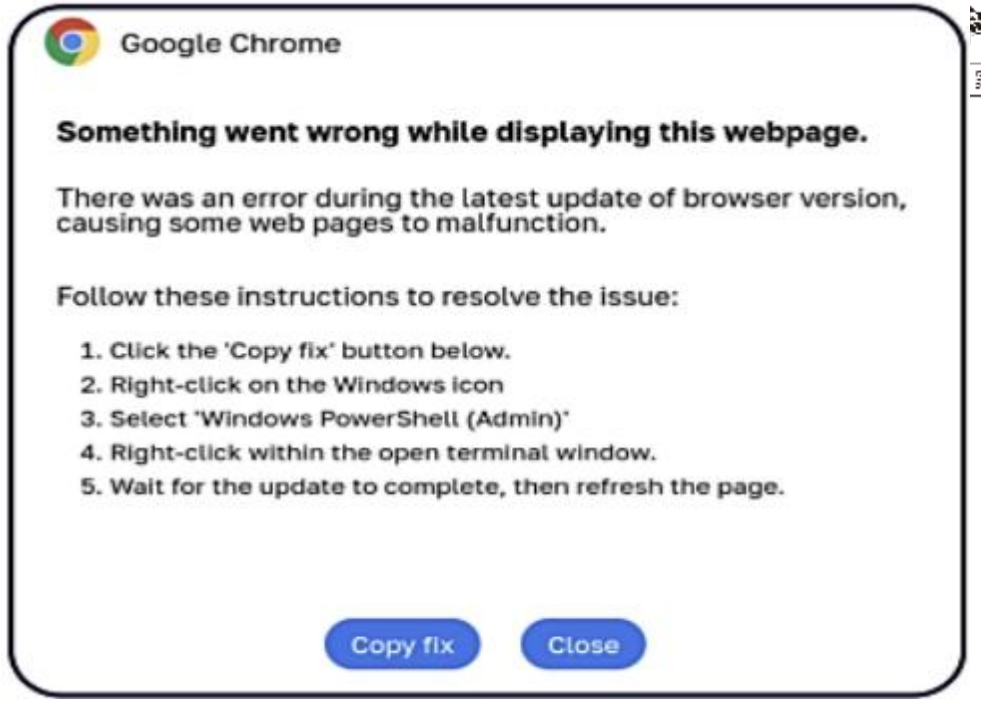
釣魚服務平台(Phishing as a Service/PhaaS)



社交工程常見手法

CkickFix

- 跳出假的瀏覽器錯誤、Windows 更新失敗或藍色當機畫面，要求使用者按下「修復 (Fix)」或「複製」按鈕，此時隱藏的惡意腳本會自動複製到剪貼簿
- 要求使用者打開執行視窗（如按下 Win + R）或命令提示字元 (cmd/ PowerShell)，並要求貼上 (Ctrl + V) 執行。



社交工程常見手法

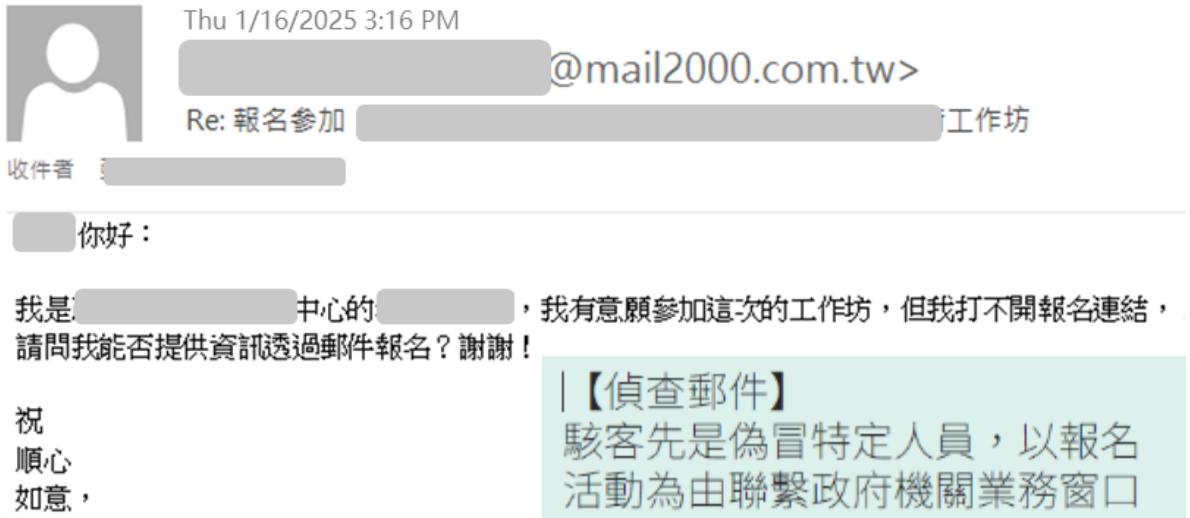
網站誘導執行惡意程式

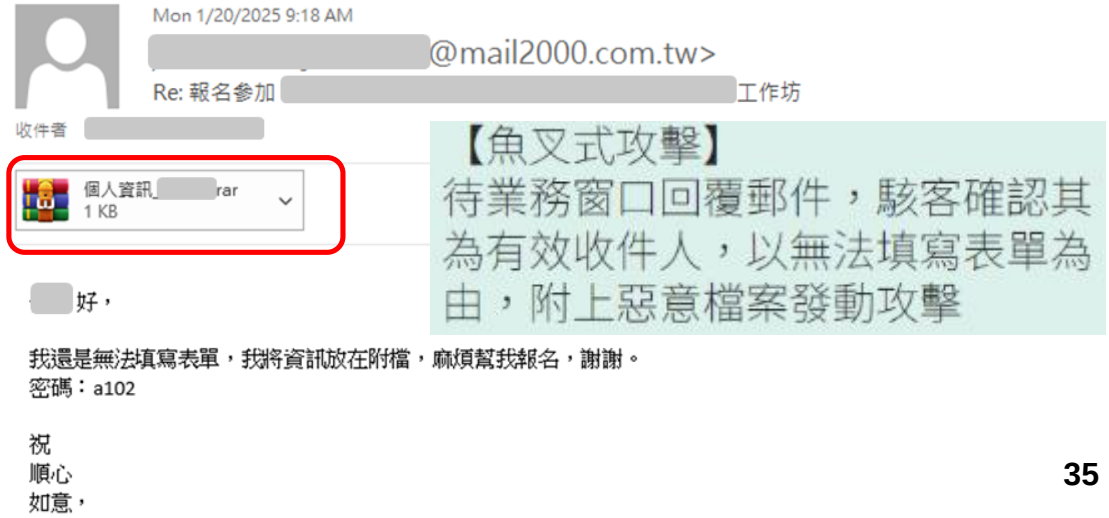
- 使用者瀏覽免費工具網站，配合網站引導進行「我不是機器人驗證」，誘導使用者手動操作執行PowerShell指令，導致使用者下載並執行竊資程式
- ClickFix的變種，都會要求使用者打開執行視窗或命令提示字元 ，並要求貼上執行。
- 建議：有要求開啟終端機、命令提示字元或PowerShell 並輸入，都要保持警覺。

社交工程常見手法

電子郵件社交工程

- 寄送與公務合作相關之正常無害電子郵件，待受駭者回覆郵件後，再寄送惡意檔案或設定雲端惡意檔案存取權限給受駭者
- 先取得受駭者信任，提高攻擊成功率
- 建議：啟動「顯示副檔名」功能辨識檔案實際類型，下載後掃毒再開啟。





釣魚郵件　偽裝成認識的人、設計吸引人的標題、偽裝成系統通知等

注意以產品報價為題之社交工程郵件

經進一步彙整分析聯防情資資訊，發現近期駭客偽稱提供業務相關產品報價，寄送內含罕見副檔名.ARJ之社交工程郵件，並將附件檔名偽裝為常見文件格式（如pdf），企圖混淆收件人判斷，點擊開啟惡意附件。當收件人執行該惡意程式後，將連線至Google雲端硬碟下載2階惡意檔案，進一步達成控制收件人電腦之目的，相關情資已提供各機關聯防監控防護建議。　資通安全網路月報（114年7月）

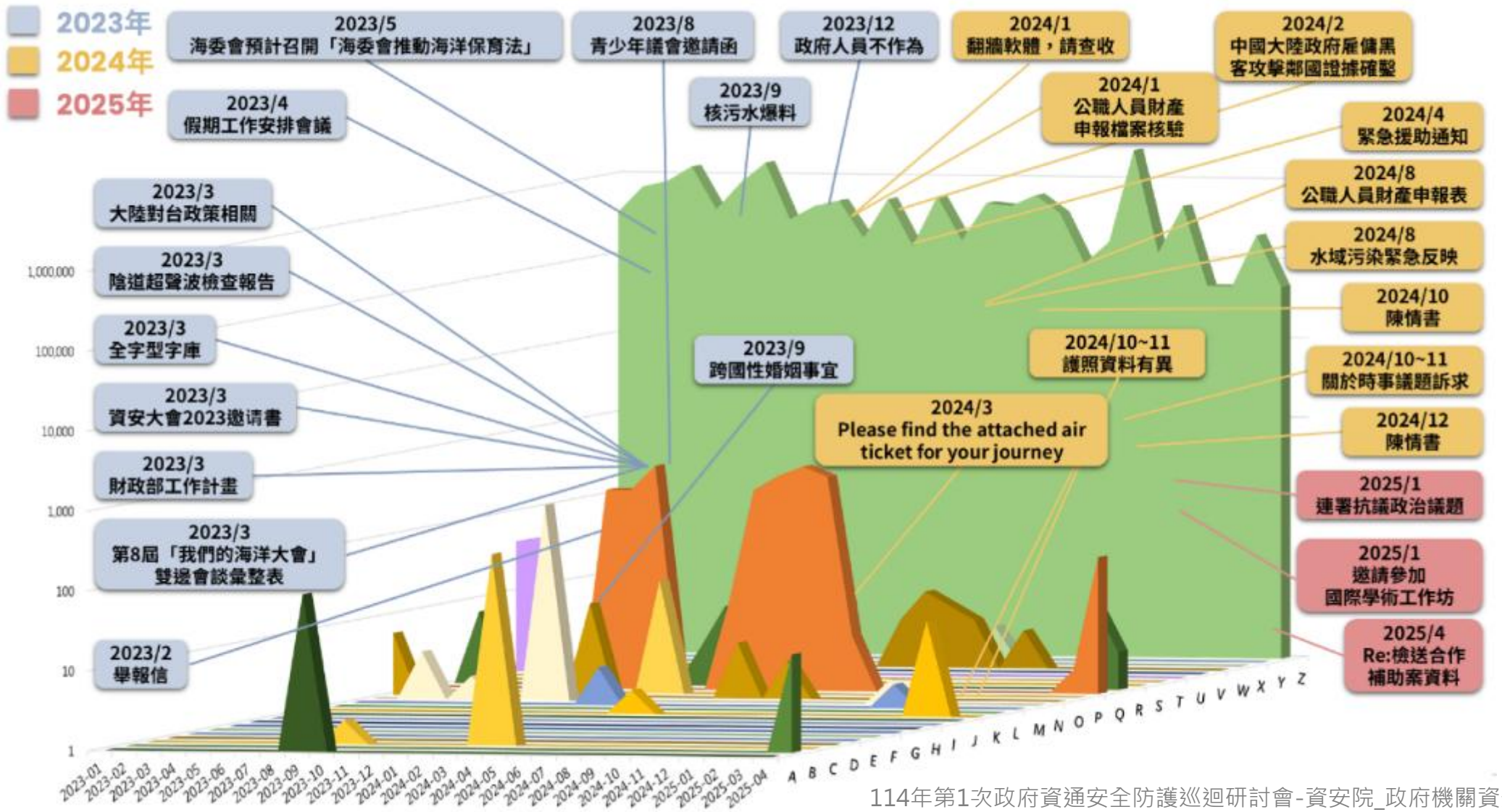
小心有關詢問志工計畫報名之惡意郵件

經進一步彙整分析聯防情資資訊，發現近期駭客利用第三方電子郵件服務(如微軟Outlook與Google Gmail)，以詢問志工計劃報名為由，針對政府機關人員寄送內含惡意附檔之社交工程電子郵件，企圖誘騙收件人開啟惡意附檔以植入後門程式，進而竊取電腦機敏資訊，相關情資已提供各機關聯防監控防護建議。　資通安全網路月報（114年8月）

小心陳情附件！偽冒PDF捷徑檔暗藏惡意程式

國家資通安全研究院發現部分機關資訊設備對外惡意連線，經機關調查顯示入侵來源為官方網站提供之陳情管道，承辦人員為處理陳情案件，將其所附之壓縮檔解壓縮後逐一檢視檔案，執行偽冒PDF檔之捷徑(lnk)檔，以致遭植入惡意程式。　資通安全網路月報（114年9月）

近3年惡意電子郵件分析



詐騙信件也吹復古風?


assword Reset Request
Microsoft <norepl @rnicrosoft.com>
To
rnicrosoft.com
就算沒有老花也難以看出!

商業電子郵件(BEC)

BEC 特色

1. 不包含惡意軟體、連結或附件
2. 針對組織內的特定人進行
3. 高度客製化

- 加入了深偽(DeepFake)技術，使整個騙局更加真實。

DeepFake? 沒錯，這就是騙術

影片連結：https://www.youtube.com/watch?v=jMJqZkFli10

我可以做些什麼

1. 【**閱讀媒體選擇**】**請避免使用手機收信**，因為看不到寄件者完整郵件地址
2. 【**信件自動預覽**】選擇關閉，使用網頁版亦同。信件閱讀選擇純文字瀏覽。
3. 【**封鎖外部圖檔**】選擇全部封鎖並勾選內文圖片要封鎖
4. 【**與業務無關**】請特別注意這類信件，盡量避免開啟
5. 【**附件檔案格式**】警惕檔案的真實格式，如.zip、.exe、.scr
6. 【**永遠零信任**】求證一定要由己方進行

圖：桃園監理站臉書

找個厲害的平台先幫我看看

Virus Check及VirusTotal平台都可以透過上傳檔案的方式，掃描檔案是否帶有惡意程式，不過還是要注意，避免機敏/機密資料外流風險。

臺南大學資訊網 – 社交工程宣導

網址：**https://www.nutn.edu.tw/cc/emailse/about.html**

»教育部115年臺灣學術網路防範惡意電子郵件社交工程演練：
115年4月-12月，期間進行2次演練。請教職員生留意個人電子郵件。

AGENDA

1. 近期資安威脅概述
2. 常見的網路攻擊態樣
3. 社交工程攻擊與防範
4. 保護智慧財產權、ODF開放文件應用、資通安全政策宣導

BCCS 漢昕科技
-能你最近的資安專家-

認識智慧財產權

- 又稱為無形或無體財產權
- 智慧財產權保障由「專利法」、「商標法」、「著作權法」與「營業秘密法」等法律分別就不同的智慧財產權加以保護。

https://lawplayer.tw/blog/p/intellectual-property-rights

保護智慧財產權

1. 不使用未經授權之電腦軟體。
2. 不違法下載、拷貝受著作權法保護之著作。
3. 未經著作權人同意，不可將受保護之著作上傳於公開之網站上或任意轉載。
4. 其他可能涉及侵害智慧財產權之行為。

https://www.nutn.edu.tw/copyright/index.htm

國立臺南大學智慧財產權宣導作業

國立臺南大學智慧財產權宣導作業管理系統，相關經濟部智慧財產局智慧財產權保護宣導與公告資料，請瀏覽參閱。

網址：
https://system.nutn.edu.tw/copyright/index.htm

https://www.nutn.edu.tw/copyright/index.htm

ODF開放文件應用宣導說明

- 為引導公務機關從文件製作、保存均以開放文件格式(ODF)處理，且使政府ODF文件能跨機關流通
- 適用windows、MacOS及Linux系統
- 數發部ODF文件應用工具說明與下載：https://moda.gov.tw/digital-affairs/digital-service/app-services/248

臺南大學資訊安全政策與目標

資安政策

確保及維持本校資訊資產之機密性、完整性與可用性，落實資通安全防護措施，以符合相關法令規範及內、外部關注方之資通安全期望與要求。

政策目標

- 本校核心資通系統的網路機房維運服務達全年上班時間 96%以上之可用性。因資通安全事件/異常事件/其他安全事故造成系統、主機異常而中斷營運服務之情事，每次最長不得超過系統所訂之復原時間目標(RTO)。
- 本校核心資通系統服務達全年上班時間 98%以上之可用性，本校核心資通系統因資通安全事件/異常事件/其他安全事故造成系統、主機異常而中斷營運服務之情事，每次最長不得超過系統所訂之復原時間目標(RTO)。

臺南大學資訊安全政策與目標

國立臺南大學資通安全管理政策、詳細的資通安全宣導資訊與公告，請參考資通安全宣導網。 https://isms.nutn.edu.tw

資通訊資產盤點

資產類別	說明/舉例
人員（People / PE）	包含全體同仁，以及委外廠商。（本校管理維護資通系統人員及其主管、各單位資訊系統負責人(資安及個資業務聯絡人)及其主管及本校資訊服務委外廠商。）
文件（Document / DC）	以紙本形式存在之文書資料、報表等相關資訊，包含公文、列印之報表、表單、計畫等紙本文件。
軟體（Software / SW）	資通系統、作業系統、應用系統程式、套裝軟體等，包含原始程式碼、應用程式執行碼、資料庫等。(本校自行開發系統或委外採購(含租賃))。
通訊（Communication / CM）	網路設備、網路安全設備、提供資訊傳輸、交換之線路或服務。
硬體（Hardware / HW）	主機設備等相關硬體設施，如電腦主機、伺服器、交換器等。
資料（Data / DA）	儲存於硬碟、磁帶、光碟等儲存媒介之數位資訊。
環境（Environment / EV）	相關基礎設施及服務，包含辦公室實體、實體機房、電力、消防設施（滅火器）、監視系統（含監視器）、租賃影印機等）等。

115年各單位保有資訊資產清查盤點作業說明：https://isms.nutn.edu.tw/Page/Index/11107

大陸品牌禁止使用及採購

- 於學校委外契約或場地租借使用規定，應明訂不得使用大陸廠牌資通訊產品
- 大陸品牌包含但不限於右方列表
- 廠商貼牌換標(昇銳攝影機案)
- 採購合約的明訂與切結

海康威視 (Hikvision)	華為 (Huawei)	大疆 (DJI)
歐家控股 (OPPO)	普聯 (TP-Link)	小米 (MI)
大華 (Dahua)	中興通訊 (ZTE)	海信 (Hisense)
魅族 (MEIZU)	努比亞 (Nubia)	真我 (REALME)
騰達 (Tenda)	海能達 (Hytera)	維沃 (vivo)
TOTOLINK	福視寶 (Foscam)	SUGAR
水星 (MERCURY)	網是 (netis)	

電腦使用安全

- 使用者**離開座位**及作業環境，應隨手將個人電腦、伺服器之作業系統**登出或鎖定**電腦。
- 電腦應設定螢幕保護程式，且啓動時間應設定**不超過15分鐘**。
- 電腦**不得任意加裝與工作無關之軟體**。

密碼設定

- 複雜度：數字、英文大小寫、特殊符號
- 密碼長度：至少**8位數**，建議**12~16**位數以上(6*2、8*2)
- **避免**放桌面上、貼在螢幕、放在電腦檔案中(可以另外紙本記錄存查但請藏好)。

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

HIVE SYSTEMS

› Learn how we made this table at hivesystems.com/password

影片連結：https://www.twcert.org.tw/tw/lp-17-1-2-20.html

我只是公司小員工，密碼隨意設也沒那麼嚴重吧?

英國158年老牌物流公司KNP，在2023年6月的一次駭客行動中被發現一名內部員工使用薄弱易猜的密碼並成功入侵。駭客對整個營運系統以及系統備份進行加密，導致核心作業全數癱瘓。雖然有保險，也請了專業復原公司，但仍無力挽救，於該月底申請破產。全公司700位員工面臨失業，而主管在接受專訪的時候無奈表示：

「我沒有告訴那名密碼被破解的員工，是他導致這一切的。你說我該告訴他嗎?」

The Economic Times: How a ransomware attack crushed a 158-year-old UK firm

機密資料要保護

紙本

- 機密及敏感文件不得隨意放置，須存於安全場所並上鎖
- 敏感文件使用後作廢銷毀，不得回收再利用

電子資料

- 重要或敏感檔案要分開存放
- 設定密碼或以加密軟體保護
- 建議避免共用資料夾

紙本

綜合媒體報導，林姓女子表示日前收到果菜市場上得標菜貨，打開檢查時發現有一疊A4紙，原本想用背面空白處寫字，未料卻驚覺上面載有台南市鹽水區公所發出的函文、台南市環保局的結業證書，以及台南市社福卡申請表等文件，其中可見民眾的身份證件影本、住址、手機號碼等基本資料，讓她氣得直呼「太離譜」。

重要資料要備份

備份的重要性

- 預防重要資料或設備損壞遺失
- 防範勒索病毒
- 確保可用性

備份之方法

- 備3份
- 不同的儲存媒體(如硬碟、光碟片)
- 本機、線上儲存設備或其他伺服器等方式存放

段落結語

個人資料與個資外洩

AGENDA

1. 什麼是個人資料
2. 為什麼需要做好個資管理與保護
3. 如何管理個資
4. 發生個資事件時，依法該怎麼處理

BCCS 漢昕科技
-能你最近的資安專家-

前言

個人資料

資訊隱私權

人格權

資訊自主權

- 是否揭露
- 時間
- 方式
- 對象
- 範圍
- 對資訊的控制

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
- 促進個人資料之合理利用

規範對象

- 公務機關
- 非公務機關：法人、自然人

保護對象

- 現存之自然人

什麼是個人資料

個人資料定義§2、§6

一般資料	特種資料	其他
• 姓名 • 出生年月日 • 身分證編號 • 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	• 病歷 • 醫療 • 基因 • 性生活 • 健康檢查 • 犯罪前科	• 其他得以直接或間接方式識別該個人之資訊

個資法規範的行為與當事人權利

請求查詢 | 請求複本 | 請求更正 | 請求停止 | 請求刪除

尊重權益 | 誠實信用
目的明確 | 正當合理

安全維護

資料合法使用

蒐集的告知義務

蒐集

直接蒐集§8、間接蒐集§9

- 機關名稱
- 蒐集目的
- 個人資料之類別
- 資料利用之期間、地區、對象及方式
- 當事人之權利及行使方式
- 得選擇性提供時，不提供將對其權益造成之影響
- 告知其個人資料之來源

蒐集

3.Shopee會蒐集哪些個人資料？

3.1 Shopee會在使用本服務的必要範圍內蒐集使用者的個人資料，包括但不限於：

1. 姓名；
2. 電子郵件地址；
3. 出生日期；
4. 帳單及/或寄送地址；
5. 銀行帳戶和付款資訊；
6. 電話號碼；
7. 性別；
8. 與您用來存取
9. 與您的人際
   有關的資訊；
10. 您的照片、
11. 基於我們的
    欺等目的所要
12. 行銷及通訊
    我們的服務
13. 使用及交易
    關的產品或

17. 前述資料，依據法務部頒佈之「個人資料保護法之特定目的及個人資料之類別」，本公司蒐集、處理、利用及保有您個人資料之種類列示如下：
18. C001 辨識個人者。(例如：姓名、職稱、住址、工作地址、以前地址、住家電話號碼、行動電話、網路平臺申請之帳號、會員編號、通訊及戶籍地址、電子郵遞地址及其他任何可辨識資料本人者等。)
19. C002 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碼、個人之其他號碼或帳戶等。)
20. C003 政府資料中之辨識者。(例如：身分證統一編號、護照號碼等。)
21. C011 個人描述。(例如：年齡、性別、出生年月日、出生地、國籍等。)
22. C031 住家及設施。(如：住所地址)
23. C034 旅行及其他遷徙細節。(例如：旅行細節)
24. C035 休閒活動及興趣。(例如：嗜好、運動及其他興趣等。)
25. C036 生活格調。(例如：使用消費品之種類及服務之細節、個人或家庭之消費模式等。)

蒐集

網站隱私權聲明

親愛的朋友，感謝您蒞臨「財政部北區國稅局全球資訊網」網站(以下簡稱本網站)，您個人的隱私權，財政所屬分局、稽徵所與服務處(以下簡稱本局)絕對予以尊重並加以保護。為了幫助您瞭解，本網站如何蒐集、護您所提供的個人資訊，請您務必詳細閱讀下列資訊：

壹、隱私權聲明適用範圍

本隱私權聲明(以下簡稱本聲明)，適用於您在瀏覽或使用本網站提供之服務時，所涉及的個人資料蒐集、處理、利用與保護，但不適用於與本網站功能連結之各政府機關網站與繳費網站。凡經由本網站連結之線上案件申請網站或繳費網站，不論是由全國各級政府機關獨立經營或是其他機關、團體、公司與本網站聯名經營，各網站均有其專屬之隱私權聲明，本網站不負任何連帶責任。當您在這些網站進行線上案件申請時，關於個人資料的保護，適用各該網站的隱私權聲明。

貳、個人資料之蒐集

一、純在本網站的瀏覽及檔案下載行為，本網站並不會蒐集任何有關個人的身分資料。

二、利用本網站所提供的各項線上申請服務時，本局會依案件辦理需求請您提供姓名、身分證統一編號/統一證號、聯絡電話、e-mail、通訊住址或戶籍地址等個人最新、最真實之資料。

三、因網路技術與網路安全管理之需要，本網站會自動記錄一些不代表您個人，但與網站使用相關之訊息，例如：使用者連線設備的IP位址等資料。

四、本網站有義務保護各申請人隱私，非經您本人同意不會自行修改或刪除任何網路民眾個人資料及檔案。除非經過您事先同意或符合以下情況始得為之：

1. 保護或防衛相關網路民眾的權利或所有權。
2. 為保護本網站各相關單位之權益。

財政部北區國稅局
National Taxation Bureau of the Northern Area, Ministry of Finance

iRent蒐集過多個資 公路局要求補正

2025/1/8 20:40（1/9 09:57 更新）

除了蒐集過多資訊，該資訊的分享及利用對象包含關係企業及未來合作對象!

公路局：合理性與必要性並不明確

（中央社記者余曉涵台北8日電）消基會昨天質疑，和運公司iRent租車條款蒐集的個資過多，分享及利用對象包含關係企業及未來合作對象，恐涉違法。公路局8日前往行政稽查後，要求和運公司補正相關佐證資料。

消基會質疑和運公司iRent租車條款蒐集的個資過多，除了姓名、電話、駕照，還有配偶個資等，範圍過大，分享及利用對象包含關係企業及未來合作對象，恐涉違法，應立即強制刪除。

交通部公路局台北市區監理所8日聯合資訊、政風及委外資訊廠商達文西個資暨高科技法律事務所等相關人員，對和運公司進行行政檢查。

公路局8日晚間發布新聞稿表示，針對和運公司將消費者個人資料分享給關係企業使用部分，雖有經當事人同意，但其合理性與必要性並不明確，為避免爭議，和運公司承諾立即將消費者個人資料上傳至其集團內共同行銷資料系統功能關閉。

https://www.cna.com.tw/news/ahel/202501080396.aspx

個人資料的合法利用

利用

目的外的使用§6、§16、§20

- 法律明文規定
- 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
- 有利於當事人權益
- 經當事人同意
- 基於公共利益為統計或學術研究，且資料無從識別特定之當事人

個人資料的合法利用

利用

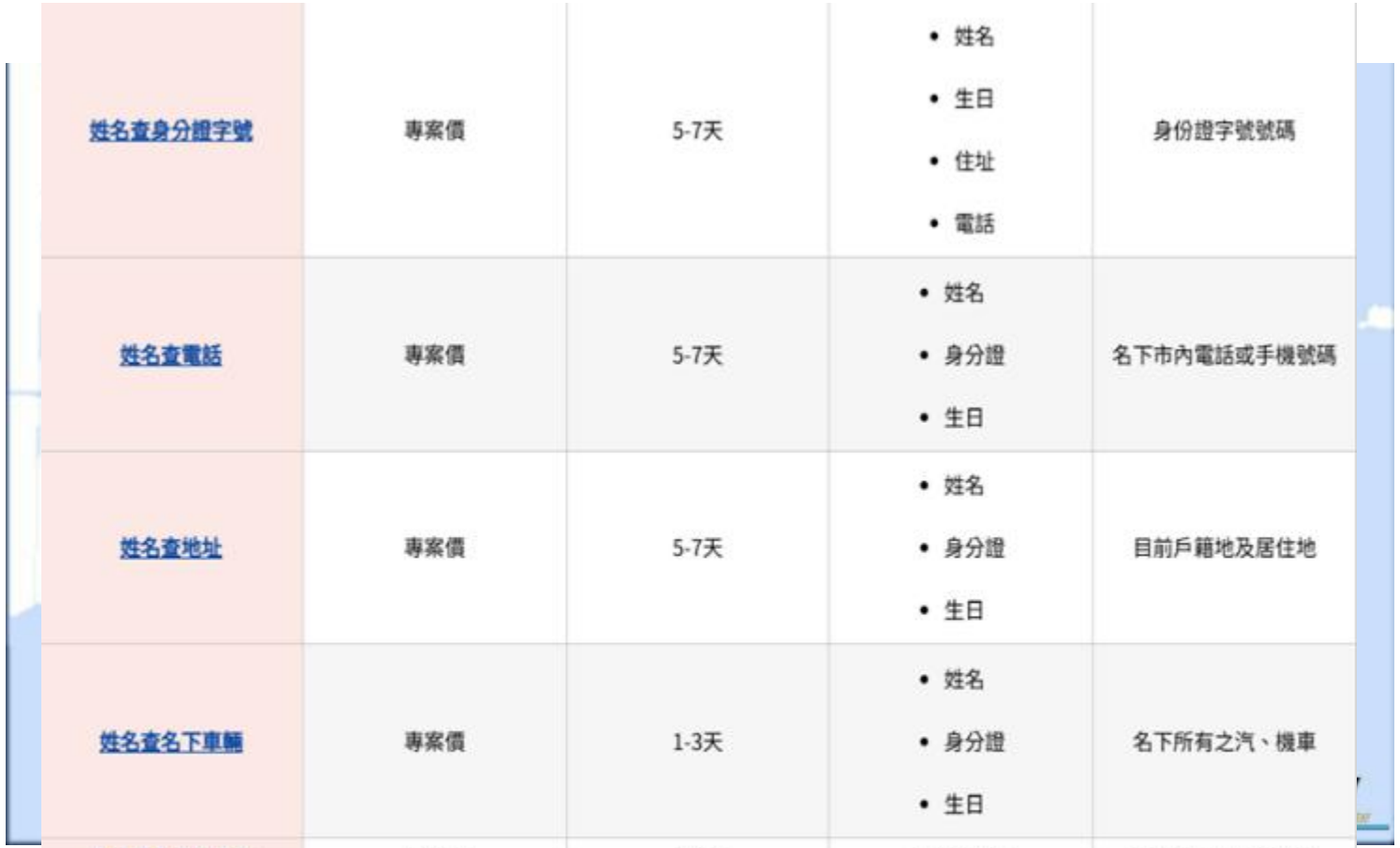
按個資法第 16 條但書第 2 款規定「公務機關對個人資料之利用，…應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。但有下列情形之一者，得為特定目的外之利用：…二、為維護國家安全或增進公共利益所必要。」；同法第 5 條規定「個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之…」。查警察機關溯源追查供毒網絡，固屬維護國家安全與增進公共利益之目的，然本件「社會安全網－關懷 e 起來通報平台」所蒐集之施用毒品等兒少個案資料，原係為協助兒少後續就醫、保護、安置或為其他必要處置，如將相關資料做上述目的外之利用，使原應受保護、關懷之兒童少年成為警察機關之關注對象，除可能妨礙兒少權益保障之原始目的達成外，亦與個人資料之利用應符合誠實信用方法之原則有間，尚難認符合個資法第 5 條之規定。

另少年事件處理法第 2 條規定，本法所稱少年係指 12 歲以上 18 歲未滿之人，為保障少年隱私權以維護其權益，同法第 83 條之 1 規定，少年之前案紀錄及有關資料應予塗銷，且原則不得提供予其他機關，依舉重以明輕之法理，其他非屬前案紀錄之資料，以及 12 歲以下兒童之資料更應予以保護，不宜提供予警察機關偵辦他案使用，併予敘明。

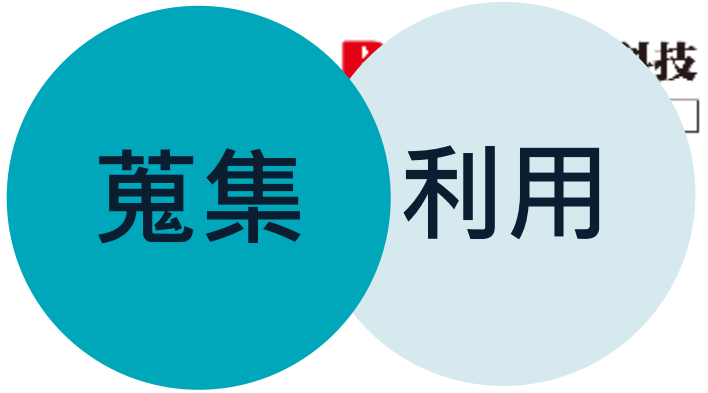
要旨：公務機關原基於特定目的所蒐集之個人資料，如欲作特定目的外之利用，須符合個人資料保護法第 16 條但書各款之一規定，並應尊重當事人之權益，依誠實及信用方法為之。

國家發展委員會發法字第1090011600號

我的個人資料變成別人的賺錢工具



姓名查身分證字號	專案價	5-7天	• 姓名 • 生日 • 住址 • 電話	身份證字號號碼
姓名查電話	專案價	5-7天	• 姓名 • 身分證 • 生日	名下市內電話或手機號碼
姓名查地址	專案價	5-7天	• 姓名 • 身分證 • 生日	目前戶籍地及居住地
姓名查名下車輛	專案價	1-3天	• 姓名 • 身分證 • 生日	名下所有之汽、機車
身份證字號查地址	專案價	5-7天	身份證字號	目前戶籍地及居住地
身份證字號查姓名	專案價	5-7天	身份證字號	現在姓名
身份證字號查電話	專案價	5-7天	身份證字號	名下市內電話或手機號碼
身份證字號查照片	專案價	5-7天	身份證字號	個人照片
身份證字號查名下車輛	專案價	5-7天	身份證字號	名下所有之汽、機車



114年6月份破獲

外洩筆數高達 9300 萬筆，包含姓名、電話、住址等敏感資訊

https://tyenews.com/2025/07/912574/

經濟合作暨發展組織(OECD)

隱私權及個人資料保護的8大原則

- 限制蒐集原則
- 品質確保原則
- 目的明確原則
- 限制目的外使用原則
- 安全確保原則
- 公開原則
- 個人參與的原則
- 責任明確原則

113年數位發展部資通安全署保有個人資料檔案公開項目彙整表

編號	個人資料檔案名稱	保有依據	特定目的	個人資料類別	作業單位
1	行政院國家資通安全會報委員名單	數位發展部資通安全署組織法第2條、數位發展部資通安全署處務規程第5條、行政院國家資通安全會報設置要點	○七五 科技行政	C○○一 辨識個人者、 C○三八 職業	綜合規劃組
2	數位發展部補助地方政府強化資通安全防護作業計畫聯絡人資料	數位發展部資通安全署組織法第2條、數位發展部資通安全署處務規程第5條、數位發展部補助地方政府強化資通安全防護作業要點第5點	○七五 科技行政	C○○一 辨識個人者、 C○三八 職業	綜合規劃組

https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

AGENDA

1. 什麼是個人資料
2. **為什麼需要做好個資管理與保護**
3. 如何管理個資
4. 發生個資事件時，依法該怎麼處理

BCCS 漢昕科技
-能你最近的資安專家-

為什麼需要做好個資管理與保護

106年發生個資事件

消基會一審敗訴!
因為雄獅有善盡法規範之善良管理人義務

https://www.consumers.org.tw/product-detail-2509325.html

112年再度發生個資事件，被主管機關裁罰

本資料由 (上市公司) 2731 雄獅 公司提供

	發言日期	113/01/17	發言時間	19:35:07
主旨	公告本公司受交通部裁罰案之說明			
符合條款	第	26	款	事實發生日 113/01/17
說明	1.事實發生日:113/01/17 2.違規情形:依據交通部113年1月12日交授觀業字第1133000076號函所諭，就本公司112年11月20日遭受網路駭客攻擊，致發生該次資安事件，違反個人資料保護法第27條第1項。 3.罰鍰金額:新臺幣200萬元 4.該主管機關之處分情形:核處新臺幣200萬元。 5.預計改善措施:本公司已就既有資安機制進行優化與落實，強化公司資訊安全系統，並遵循主管機關之相關專業建議。			

主管機關直接罰到最重，限期不改正，最高可罰到1500萬

史上最大規模個資外洩事件-11.7億美元的代價

酷澎透過數位指紋及其他鑑識證據，確認外洩用戶資料之涉案者為一名前員工，該涉案者已坦承相關行為，並詳細說明其存取用戶資料的手法。初步結果顯示，該涉案者雖曾利用竊取的內部安全金鑰，存取約3300萬個帳戶的基本用戶資料，但實際僅保留約3000個帳戶的資料，且相關資料已在事件曝光後全數刪除。

酷澎進一步說明，涉案者所保留的資料內容，僅包含姓名、電子郵件、電話號碼、地址及部分訂單紀錄，其中涉及的大樓門禁密碼2609組；整起事件中，未包含任何付款資訊、登入憑證或個人報關號碼，亦未有任何資料被傳送予第三方。

1.祭出補償方案： 台灣酷澎將直接通知受影響的台灣客戶，且提供總金額超過新台幣2億元的補償方案，每位受影響的客戶將獲得總價值新台幣1,000元的酷澎購物折價券。預計自今年3月8日起陸續發放。 coupang newsroom

https://ec.ltn.com.tw/article/breakingnews/5289937

AGENDA

1. 什麼是個人資料
2. 為什麼需要做好個資管理與保護
3. **如何管理個資**
4. 發生個資事件時，依法該怎麼處理

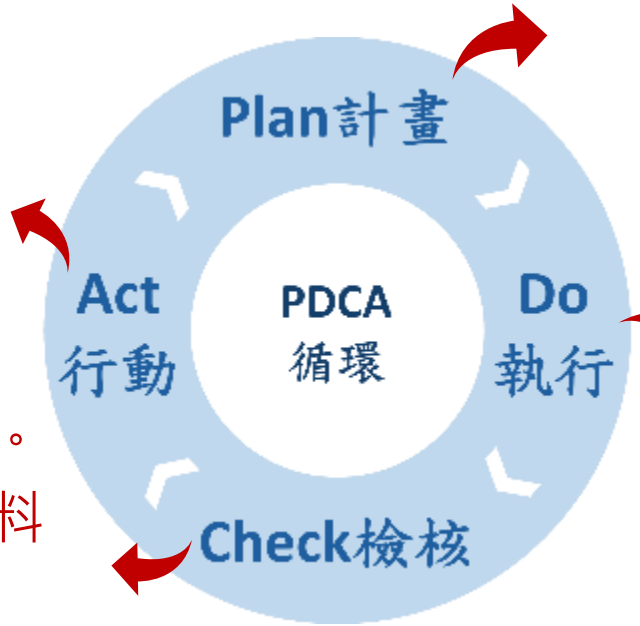
BCCS 漢昕科技
-能你最近的資安專家-

適當之安全維護措施

措施種類(細則§12)

- 組織上措施
- 技術上措施

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。
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。

什麼都查不到，麻煩就大了

蝦皮

- 個資盤點上仍僅提供4筆盤點內容
- 針對風險評鑑結果未提供已採取之矯正措施
- 委外廠商未落實稽核，未能提供完整的安全管控執行、稽核紀錄

20萬 +20萬

誠品

- 帳號管理執行未確實
- 要求補正之個資盤點資料仍不完整
- 委外廠商監督管理未落實執行

10萬 +10萬

旋轉拍賣

- 佐證強化網站防詐警示、登入採用雙重驗證機制、禁止用戶利用對話功能傳送未經驗證之網址連結等資安措施
- 惟未提供針對委外廠商整體制度稽核，尚有待改進之處

限期改正

2023年蝦皮、誠品生活及旋轉拍賣接連發生個資外洩事件

先知道有哪些--個資盤點表欄位範例

單位名稱、保管人/資料建立者	蒐集/處理/利用個資之 法律依據 + 特定目的
流程名稱、個人資料檔案名稱	個資類別、特種個資及蒐集依據
個人資料檔案之用途或說明	蒐集/處理/利用之方法與範圍
個資檔案儲存類型、可否公開	個資刪除/生命週期之軌跡紀錄

才知道如何分配保護資源--個資風險評鑑範例

	個資類型		風險評估機制					風險管理機制		
名稱	分類項目		個資價值(A)			相關指標(B)	風險值	儲存方式	有存取權限者	因應措施
說明	當事人	類型	當事人評分： • 校內員工(1) • 學生(2)	類型評分： • 一般(1) • 財務(2) • 特種(3)	價值結論： 當事人評分 + 類型評分	• 外洩可能性(1~3) • 衝擊值(1~4)	A x B	紙本、數位、雲端、以上皆是	誰有權限存取個資	權限限制
舉例	校內員工	薪資資料	1	2	1+2=3	1+2=3	3*3=9	紙本、本地資料庫	人事、出納	資料庫權限設定、紙本專人保管
	學生	聯絡資料	2	1	2+1=3	1+1=2	3*2=6	雲端資料庫	校內各單位	雲端權限設定
	學生	獎學金資料	2	2	2+2=4	1+1=2	4*2=8	紙本、本地資料庫	教務、學務、出納	資料庫權限設定、紙本專人保管

安全維護措施的最高指導原則

AGENDA

1. 什麼是個人資料
2. 為什麼需要做好個資管理與保護
3. 如何管理個資
4. **發生個資事件時，依法該怎麼處理**

BCCS 漢昕科技
-能你最近的資安專家-

事件發生了，記得通知當事人

使當事人知悉或可得知悉之方式為之

LV遭竊個資包含：姓名、性別、國家、電話號碼、電子郵件、郵寄地址、出生日期、購買偏好資料、護照號碼


親愛的客戶，

我們很遺憾地通知您，有一未經授權的第三方短暫進入了我們的系統，並取得了您部分的資訊。

我們想向您確保，被進入的資料庫中並未包含任何密碼或財務資訊，例如信用卡資訊、銀行資料或其他金融帳戶資訊。

在Louis Vuitton，我們高度重視您對我們的信任以及我們之間關係的保密性。因此，此事件現已獲得控制，我們已進一步強化系統防護，並已聘請資安領域的頂尖專家進行合作。

發生個資事件，應採取適當應變措施，以適當方式通知當事人，並研討預防機制避免再度發生。

噓! 不要跟別人說，公司發生個資外洩了...

本資料由　(上市公司) 2762 世界健身-KY　公司提供

序號	2	發言日期	113/06/21	發言時間	21:14:57
[redacted]					
主旨	(更正格式)本公司之子公司及子公司代表人接獲 教育部裁處書乙案				
符合條款	第	26	款	事實發生日	113/06/21
1.事實發生日：113/06/21 2.事實發生主體：代子公司申報：香港商世界健身事業有限公司 3.發生緣由(事件說明)：本公司之子公司香港商世界健身事業有限 教育部6月19日發函，以子公司違反個人資料保護法第12條、 第27條第1項及個人資料保護法施行細則第12條第2項規定裁處。 4.處理過程：本公司已針對此事件進行檢討，並已全面加強資訊安 未來將持續強化以確保資通安全。 5.處分情形：子公司及子公司代表人皆受罰鍰新臺幣140萬元。					

12條說，發生個資外洩事件，應查明後通知當事人；
27條(修法已刪除)說，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。

未採行適當之安全措施，而且未告知當事人!!

違反個資法的罰則

民事

如被害人不易或不能證明其實際損害額時
每人每一事件NT$500~NT$20,000
同一件事造成多數當事人權利受侵害，合計最高總額2億元為限

刑事

5年以下有期徒刑、拘役或科或併科新臺幣一百萬元以下罰金

行政處罰

200萬元罰緩並限期改正，未改正者，依所違反之事項處
最高1500萬元罰緩
非公務機關之代表人並受同一額度罰鍰之處罰

臺南大學個資安全政策

個資政策

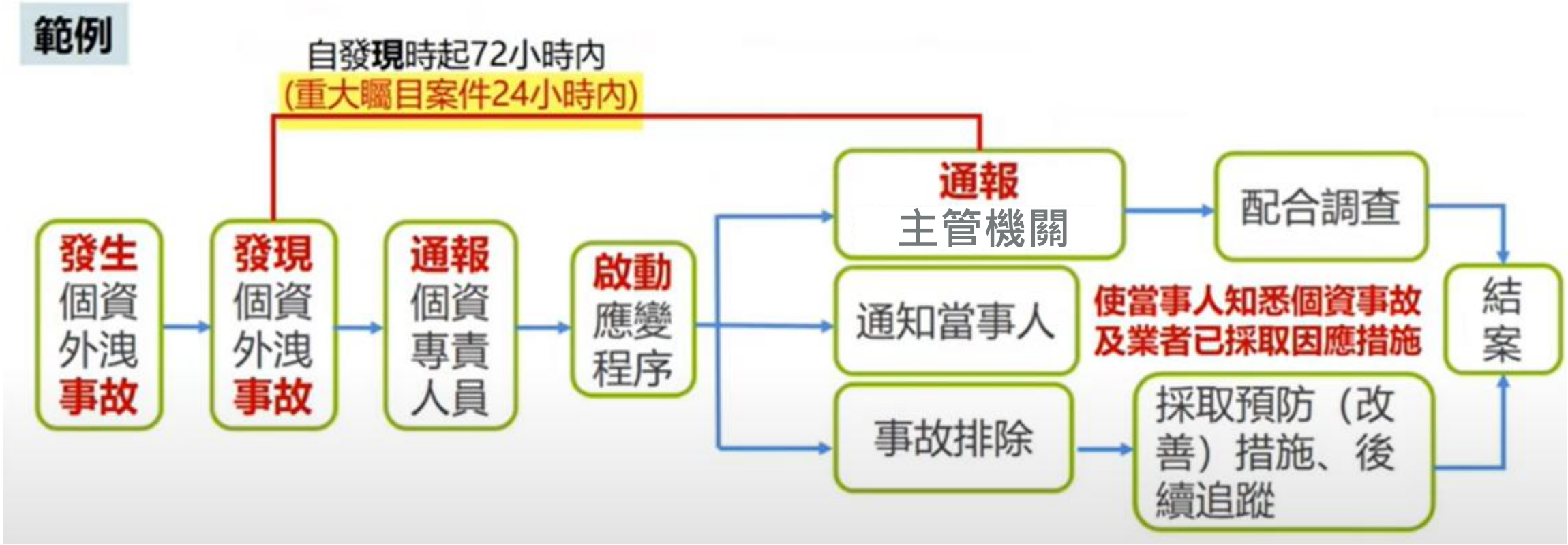
落實個人資料之保護及管理並符合個人資料保護法之要求。

政策目標

- 依據相關法律規範，保護個資之蒐集、處理、利用、儲存、傳輸、銷毀，使其免於內外在威脅導致之竊取、竄改、毀損、滅失或洩漏等風險
- 透過教育訓練提升同仁對個資保護之安全意識與管理能力
- 定期進行風險評鑑，降低營運風險，創造個資及隱私保護環境

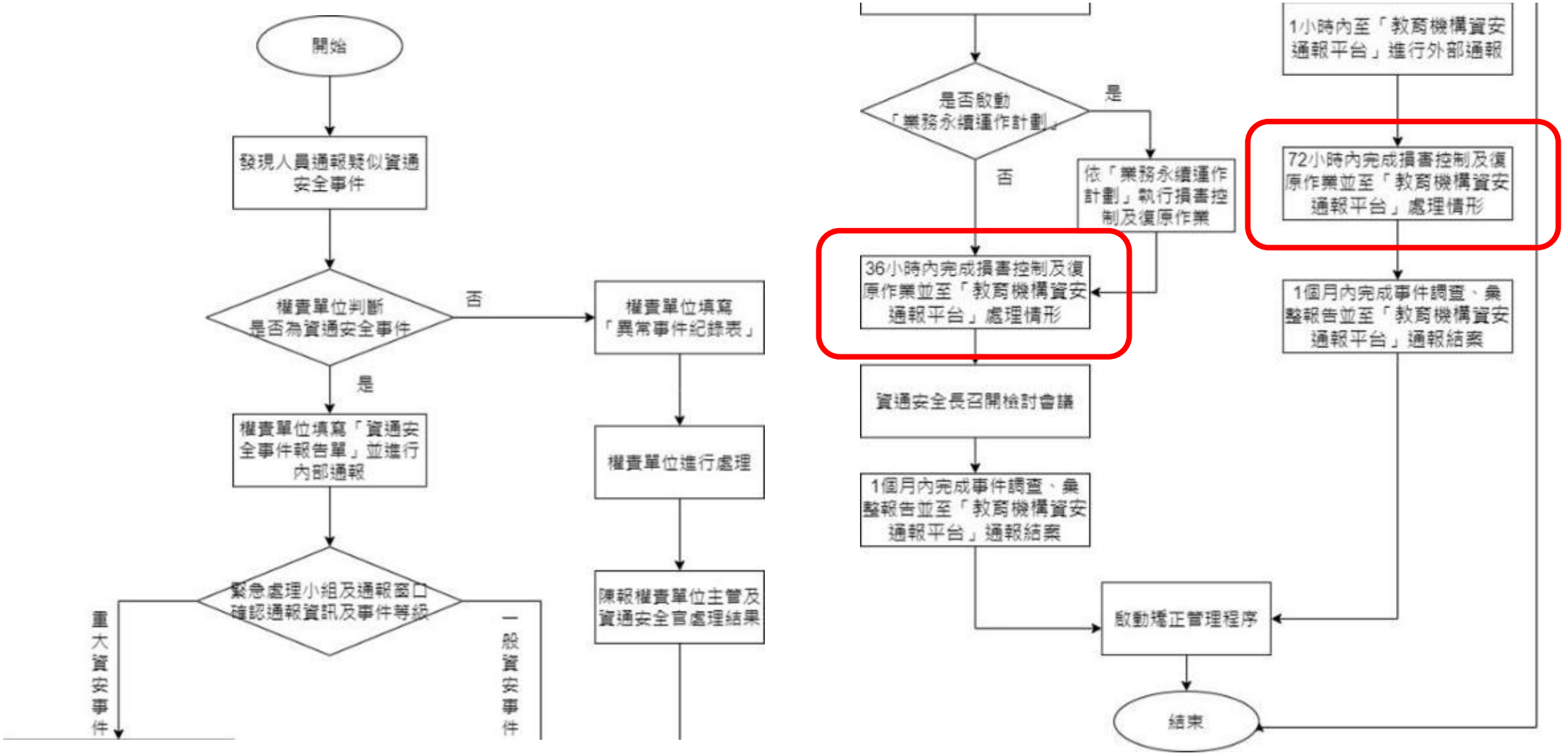
個資事件通報流程

I 通報及應變程序(事故因應流程之文字或程序圖)



資策會科技法律研究所影片提供

資安事件通報流程


開始
發現人員通報疑似資通安全事件
權責單位判斷是否為資通安全事件
否
是
權責單位填寫「異常事件紀錄表」
權責單位填寫「資通安全事件報告單」並進行內部通報
權責單位進行處理
緊急處理小組及通報窗口確認通報資訊及事件等級
陳報權責單位主管及資通安全官處理結果
重大資安事件
一般資安事件
是否啟動「業務永續運作計劃」
是
否
依「業務永續運作計劃」執行損害控制及復原作業
36小時內完成損害控制及復原作業並至「教育機構資安通報平台」處理情形
資通安全長召開檢討會議
1個月內完成事件調查、彙整報告並至「教育機構資安通報平台」通報結案
1小時內至「教育機構資安通報平台」進行外部通報
72小時內完成損害控制及復原作業並至「教育機構資安通報平台」處理情形
1個月內完成事件調查、彙整報告並至「教育機構資安通報平台」通報結案
啟動矯正管理程序
結束

臺南大學個資保護宣導網

國立臺南大學個人資料保護管理政策、詳細的個人資料保護資訊與公告，請參考個人資料保護宣導網。

https://pip.nutn.edu.tw

結語-養成資安警覺心

92