

國立臺南大學

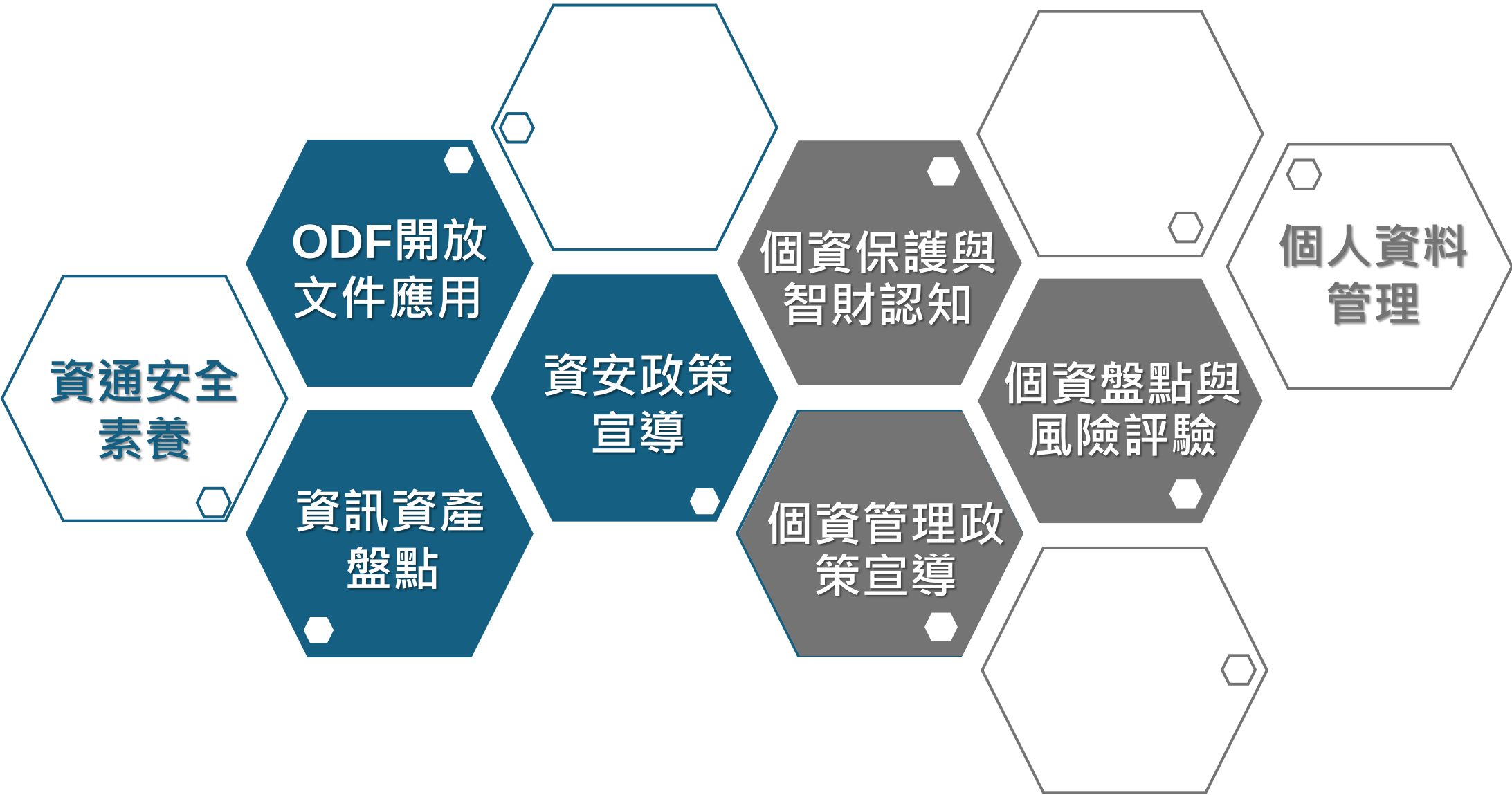
資通安全暨個資保護認知 宣導教育訓練

講者：漢昕科技 顧問 張家華

日期：115年 7 月 29 日



本次教育訓練目的





AGENDA

1

常見的網路攻擊態樣

2

辦公室實體與遠距安全

3

保護智慧財產權、ODF開放文件應用、資通安全政策宣導

4

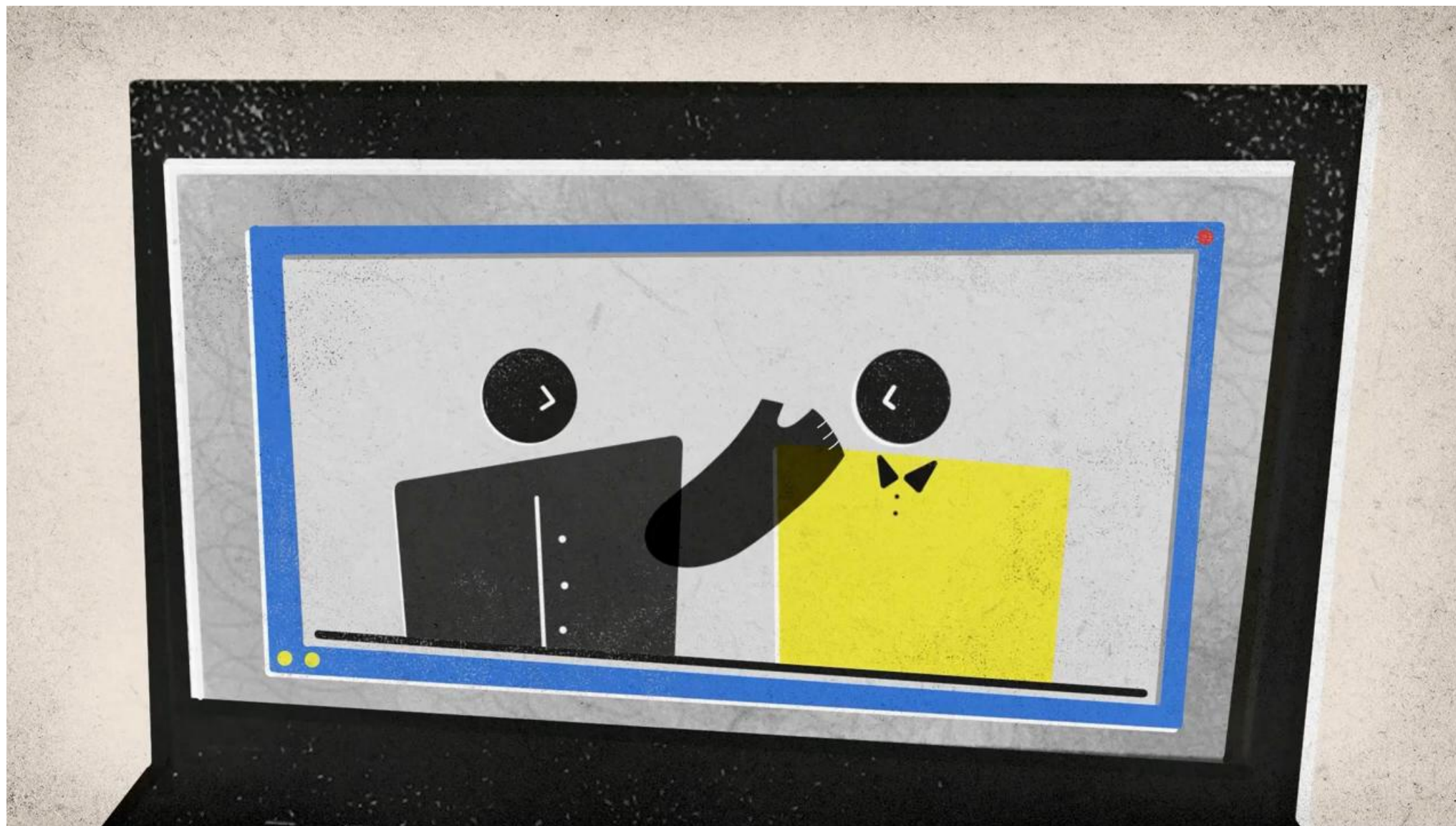
社交工程

5

個人資料保護法與實務
應用重點

6

AI 應用安全與資安防護



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」能看到資料。
- 完整性 (Integrity)：確保資料「沒被偷偷改過」。
- 可用性 (Availability)：想用資料時「隨時能用」。

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。
- 常見的攻擊的類型有以下幾種：

惡意程式

分散式阻斷服務(DDoS)

殭屍網路

勒索軟體

物聯網攻擊

網路釣魚

變臉詐騙



網路攻擊態樣



項目網路

訂單程票 ▾

Home / Order train

圖片驗證檢

請輸入圖形中的英數

7Z851

語音播放 重新產生

傳送中...

為了保障大眾訂票利益與維護訂票作業之公平性及預防程式訂票之投機行檢核方能完成訂票作業。

目前使用人數較多
為維持登入後操作體驗順暢，您即將進入
等待區

前往排隊

系統忙碌中，請稍後再試

返回

錯誤代碼：APP1029

三立新聞網

到建站

左營

重新操作。

無偏好

網路攻擊態樣

暴力攻擊

- 暴力破解帳號密碼，利用

撞庫攻擊

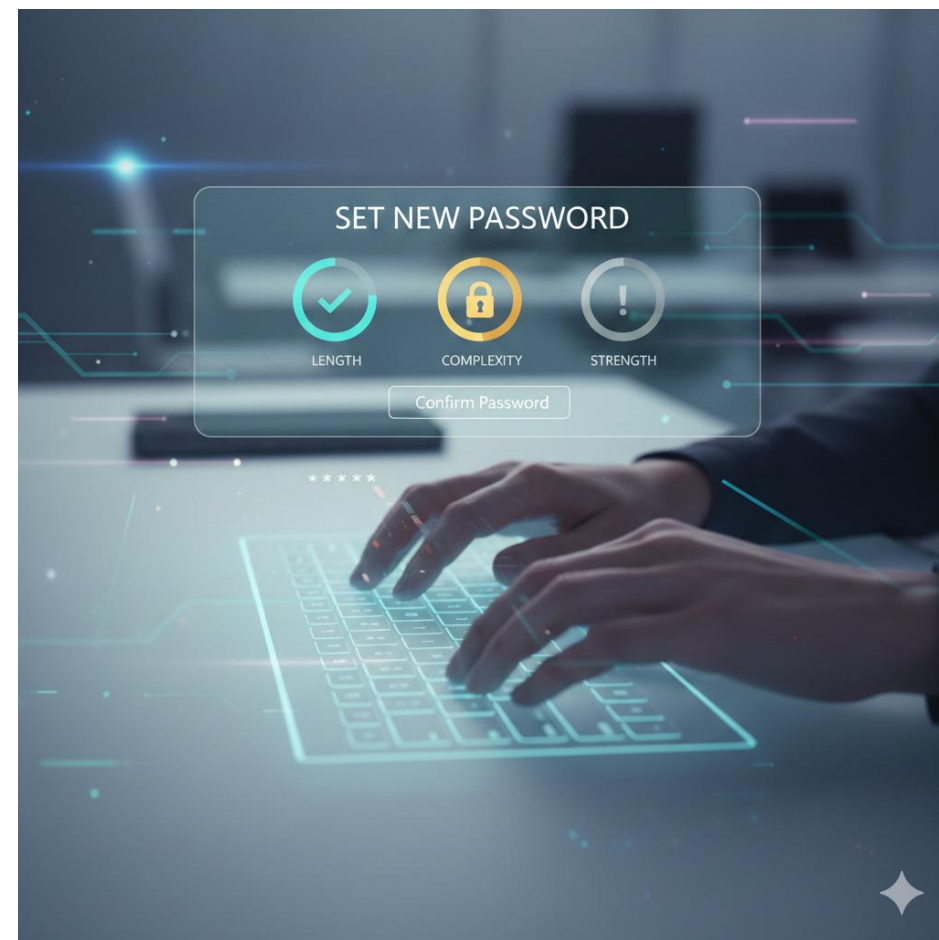
- 利用外洩的帳戶密碼，放

```
[80][http-get-form] host: 192.168.100.155 login: admin
[80][http-get-form] host: 192.168.100.155 login: admin
[80][http-get-form] host: 192.168.100.155 login: admin
[80][http-get-form] host: 192.168.100.155 login: admin
[80][http-get-form] host: 192.168.100.155 login: admin
[80][http-get-form] host: 192.168.100.155 login: admin
[80][http-get-form] host: 192.168.100.155 login: admin
[80][http-get-form] host: 192.168.100.155 login: admin
[80][http-get-form] host: 192.168.100.155 login: admin
[80][http-get-form] host: 192.168.100.155 login: admin
[80][http-get-form] host: 192.168.100.155 login: admin
[80][http-get-form] host: 192.168.100.155 login: admin
1 of 1 target successfully completed, 12 valid passwords
Hydra (http://www.thc.org/thc-hydra) finished at 2017-07-27 15:26:24
```



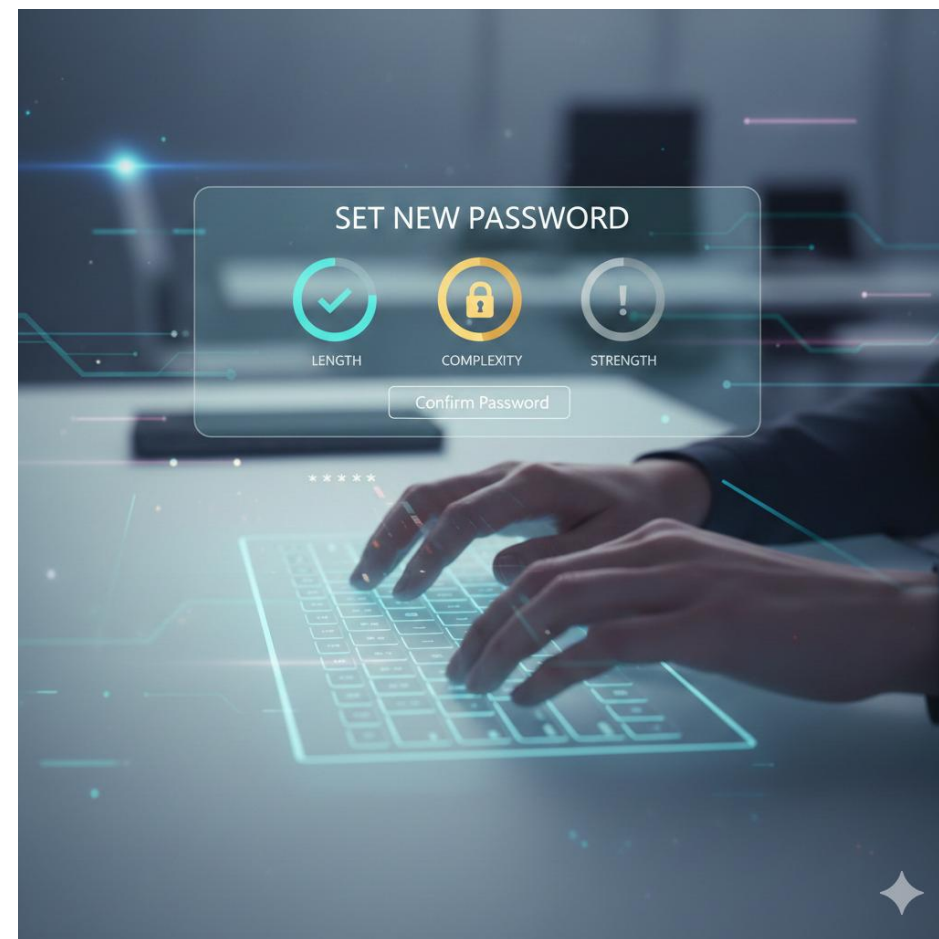
密碼設置的原則

- 使用高強度的密碼：選擇長度至少11個字符以上的複雜密碼，包括大寫字母、小寫字母、數字和特殊字符。避免使用常見的字詞、生日、姓名等容易猜測的密碼。
- 不要重複使用密碼：確保您在不同的設備和帳戶中使用不同的密碼。這樣，如果一個密碼被破解或洩漏，其他帳戶仍然保持安全。



密碼設置的原則

- 定期更換密碼：定期更改密碼是一種良好的安全習慣。根據需要，定期更換資訊和物聯網設備的密碼，例如每三個月或每六個月。



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，
- 即使成功偵測到一次惡意程式，也

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



行動裝置的資訊安全-威脅與防護

- 不明的下載來源
- 應用程式更新
- 應用程式權限要求

應用程式安全



裝置設定安全



- 密碼設定
- 避免破解行動裝置

- Wi-Fi
- 藍牙
- VPN?



連線功能安全



資料保護

- 閱讀授權聲明
- 避免非必需的授權
- 進行資料備份

數位惡夢：麗莎的意外曝光

麗莎是一位極富創意的平面設計師，她的人生大部分都離不開網路。她透過各種應用程式和網站處理銀行事務、購物和社交活動。有一天，她發現自己的銀行帳戶出現了一些奇怪的扣款——都是她從未買過、從未去過的商店裡的商品。隨後，她的社群媒體帳號開始發布垃圾訊息，推銷一些稀奇古怪的產品和服務，朋友們也反映收到了她發來的異常郵件。

麗莎意識到自己失去了對數位身分的控制權，突然陷入恐慌。她的個人照片被洩露，私人對話也被曝光。客戶開始質疑她的可靠性，她的聲譽也受到了打擊。在諮詢網路安全專家後，麗莎發現自己的密碼已被盜用。網路犯罪分子入侵了她最敏感的帳戶，一點一點地摧毀了她的數位世界。一個問題始終縈繞在她心頭：這一切究竟是怎麼發生的？

網路犯罪者的卑鄙伎倆：五種常見手段

事情經過：

麗莎收到一封看似來自她銀行的電子郵件，郵件中包含銀行的官方標誌和品牌識別。郵件聲稱她的帳戶存在可疑活動，並敦促她點擊連結驗證身份。連結指向一個虛假網站，麗莎輸入登入憑證後，網站便竊取了她的資料。

社交工程攻擊：

社交工程攻擊是指攻擊者偽裝成您認識或信任的人或事物，誘騙您做出不該做的事情。他們會發送看似合法的電子郵件或訊息，常常營造出強烈的緊迫感、恐懼感或好奇心。



雲安維運



聯防設備



風險檢測



顧問諮詢



資安學苑

網路犯罪者的卑鄙伎倆：五種常見手段

事情經過：

麗莎下載了一個她以為是正版的字體包，用於她的設計工作。然而，字體包裡隱藏著一個鍵盤記錄器，它自動安裝到了她的電腦上。隨著時間的推移，這個記錄器記錄了她多個帳戶的登入訊息，並將這些訊息發送給了攻擊者。

惡意軟體：

惡意軟體是一種旨在感染電腦的惡意程式。一旦感染，網路犯罪分子就可以為所欲為。鍵盤記錄器（有時也稱為資訊竊取程式）是一種惡意軟體，它會記錄裝置上的每個按鍵操作，包括您的登入名稱、密碼和其他敏感資料。



雲安維運



聯防設備



風險檢測



顧問諮詢



資安學苑

網路犯罪者的卑鄙伎倆：五種常見手段

事件經過：

麗莎的許多帳號都使用了像

「lisa2020」這樣簡單的密碼。

攻擊者使用軟體系統性地嘗試常見密碼，輕易破解了她的帳號。

暴力破解攻擊：

在暴力破解攻擊中，網路犯罪者使用自動化工具嘗試大量密碼組合，直到猜出正確密碼為止。弱密碼尤其容易受到這種攻擊。

網路犯罪者的卑鄙伎倆：五種常見手段

事件經過：

麗莎常用的一個社群媒體平台遭遇資料外洩。由於她在其他地方也使用了相同的密碼，攻擊者利用洩露的憑證訪問了她的其他帳戶。

資料外洩：

當網站或服務遭到駭客攻擊時，伺服器上儲存的所有帳戶都可能受到影響。如果有人有多個帳戶中使用相同的密碼，一旦其中一個帳戶的密碼洩露，該密碼就可能被用來存取受害者的其他帳戶。

網路犯罪者的卑鄙伎倆：五種常見手段

事情經過：

一名網路罪犯想在周末盡可能賺錢，於是他前往暗網購買了超過10萬個已被盜用的帳戶及其完整密碼。麗莎的其中一個帳戶就在其中。

購買憑證：

網路犯罪分子可以輕易地在網路上購買您的密碼，通常是在暗網上。某些網路犯罪分子專門竊取受害者的密碼，他們會使用我們目前討論過的任何方法。然後，他們會將竊取的密碼儲存起來，並出售給其他網路犯罪分子。

您可以採取的關鍵步驟

幸運的是，只需採取簡單的步驟，您就可以在保護您的帳戶和線上數位生活方面取得很大進展。

- 為每個帳戶設定一個長且唯一的密碼。我們建議使用密碼短語，即由多個單字組成的長密碼。
- 盡可能為最重要的線上帳戶啟用多因子身份驗證 (MFA)。

Time it takes a hacker to brute force your password in 2025

Hardware: 12 x RTX 5090 | Password hash: bcrypt (10)

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	57 minutes	2 hours	4 hours
6	Instantly	46 minutes	2 days	6 days	2 weeks
7	Instantly	20 hours	4 months	1 year	2 years
8	Instantly	3 weeks	15 years	62 years	164 years
9	2 hours	2 years	791 years	3k years	11k years
10	1 day	40 years	41k years	238k years	803k years
11	1 weeks	1k years	2m years	14m years	56m years
12	3 months	27k years	111m years	917m years	3bn years
13	3 years	705k years	5bn years	56bn years	275bn years
14	28 years	18m years	300bn years	3tn years	19tn years
15	284 years	477m years	15tn years	218tn years	1qd years
16	2k years	12bn years	812tn years	13qd years	94qd years
17	28k years	322bn years	42qd years	840qd years	6qn years

多因子身份驗證 (MFA) 安全性比較

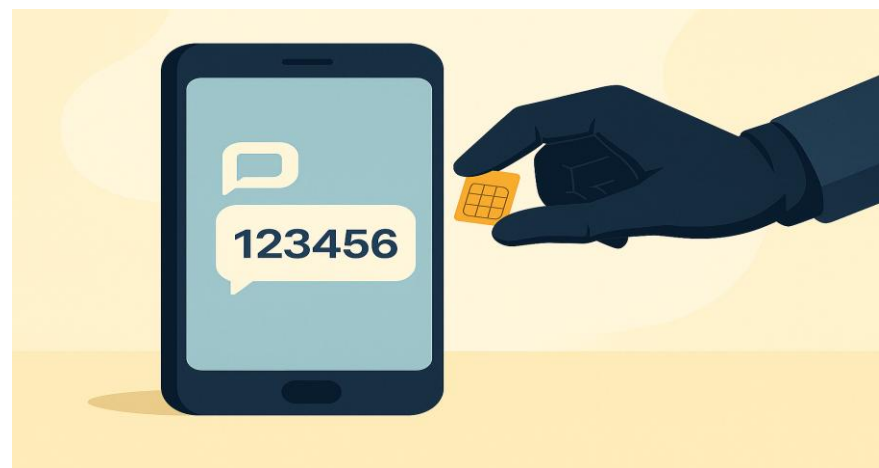
1. 簡訊驗證碼 (SMS OTP)

運作方式：將一次性密碼 (OTP) 傳送到你的手機簡訊。

風險：

- SIM卡交換 (SIM Swap) 攻擊：駭客騙過電信商取得你的號碼。
- 網路釣魚、中間人攻擊：容易被轉發。

安全性：最低。



多因子身份驗證 (MFA) 安全性比較

2. 驗證App (Authenticator App - 如 Google Authenticator)

運作方式：在App內生成 TOTP (時間型一次性密碼)，與網站同步時間。

風險：

- 釣魚攻擊：駭客可能偽裝網站騙你輸入驗證碼。
- 惡意軟體：若手機中毒，可能竊取驗證碼。

安全性：中等，比 SMS 好，因為密碼和驗證碼在不同裝置 (手機)。



多因子身份驗證 (MFA) 安全性比較

3. 硬體金鑰 (FIDO2/WebAuthn)

運作方式：基於公鑰加密，金鑰與網站直接認證，不需輸入密碼或代碼。

優勢：

- 防釣魚：金鑰認證的是真實網站，而非假網站。
- 防中間人/重放攻擊：透過加密和計數器保護。
- 無共享機密：金鑰不會在不同網站上被識別。

安全性：最高，推薦使用。



預防被釣魚網站攻擊

留意可疑的電子郵件或訊息

通知要收錢、送禮
或威脅關閉臉書帳號

臉書來自
fb.com、
facebook.com 或
facebookmail.com

絕不點擊可疑連結

自稱來自 Facebook
可疑電子郵件或訊息，

勿開連結或附件。

絕不回應此類電子郵件

跟你要帳號、密碼、
信用卡、個資

接收警告

接收不明登入的警告

開啟雙重驗證



雲安維運



聯防設備



風險檢測



顧問諮詢



資安學苑

帳號被盜急救辦法

查看郵件中是否有
帳號異動通知信

點擊信中『立即保
護你的帳號』

提示上傳個人資料
驗證

添加E-mail收取驗
證碼



雲安維運



聯防設備



風險檢測



顧問諮詢



資安學苑



AGENDA

1

常見的網路攻擊態樣

2

辦公室實體與遠距安全

3

保護智慧財產權、ODF開放文件應用、資通安全政策宣導

4

社交工程

5

個人資料保護法與實務
應用重點

任何人都可以成為視覺駭客

每天有多少訪客和承包商進出您的辦公室？甚至您自己的員工也可能看到敏感資訊。

「貼在螢幕上的密碼」

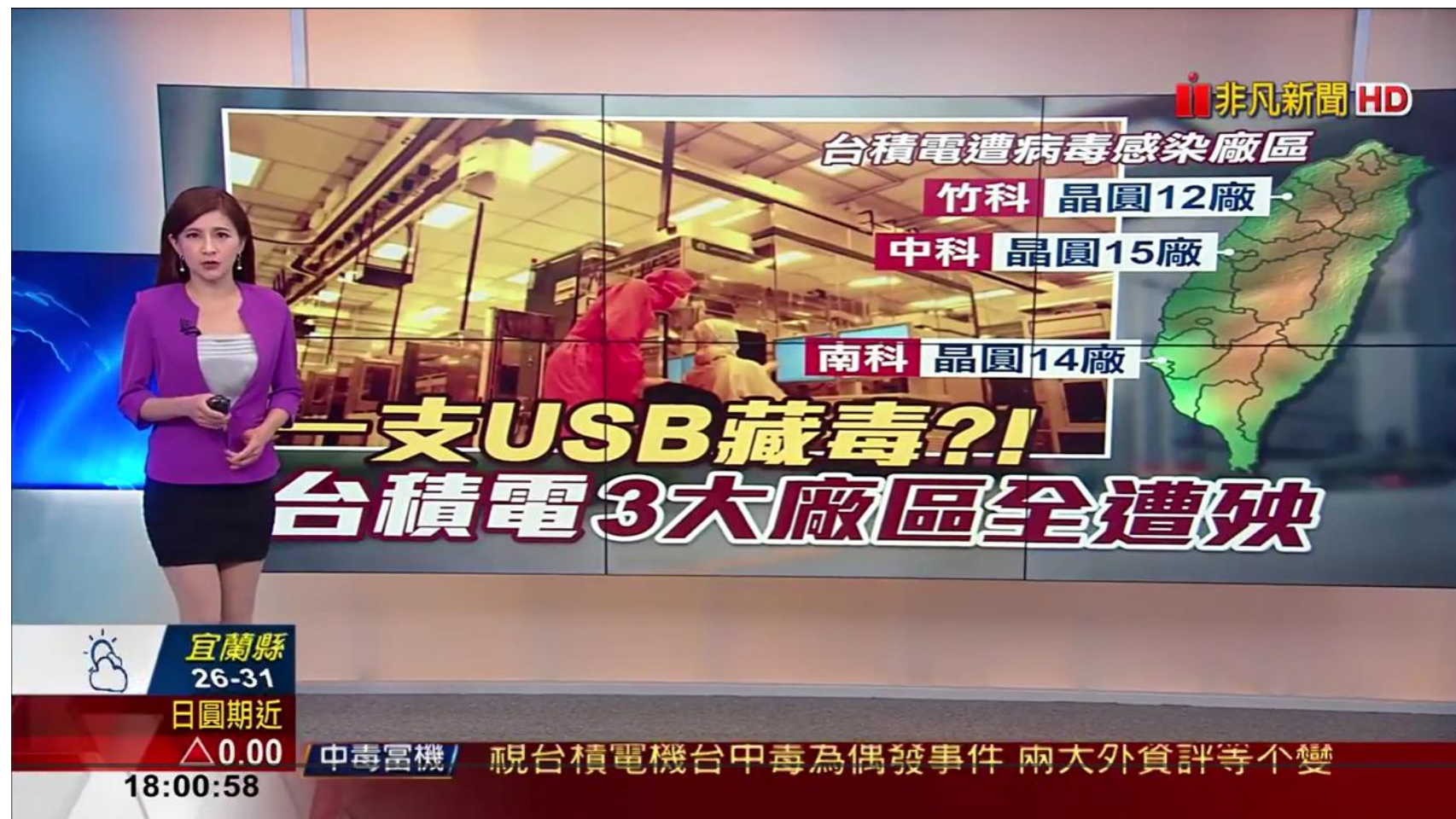
「沒拔出的隨身碟」

「白板上的會議密語」





台積電被視為是台灣最尖端科技的半導體國際大廠，卻因一個工程師面對新進機台與導入自動搬運系統，犯下疏失，從過去先隔離掃毒再連線的SOP（標準作業程序），變成先連線再掃毒，卻因此「巧合的」導致含知名勒索病毒Wanna Cry快速利用台積電最先進的全台晶圓連線管理能力，快速感染所有機台。



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」。





電子資料

中正大學學生在臉書社團「靠北中正」發文表示，通識中心的服務學習講座通知信夾帶全校學生個人資料，學校學生個資被外洩，而且電話地址統統有，直呼太扯。

中正大學主任秘書楊宇勛表示，通識中心發現時立即通知校方，確認信件無法收回後，立即發送email給收到信件的220位學生，請學生勿再將資料擴散以免觸法。另也立即開始協調避免日後再發生這樣的情形，由副校長檢視可能外洩的資料，從後端email設置關卡避免再有誤傳情形，該加密的資訊也會加密，全面防堵外洩事情再發生。



一次的資料外洩，竟然會造成這麼大的損失?!

根據IBM進行的年度資料外洩報告，
一個外洩事件平均損失**488萬美金**(NT\$1.56億)



一次的資安事件
損失也不容小覷



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，且啟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。

案例一

- 資安院發現某機關資訊設備有**竊資軟體**特徵之連線
- 機關調查發現係同仁於google搜尋**winrar破解程式**，並從搜尋結果中下載並執行了惡意程式，導致電腦受駭

案例二

- 資安院發現某機關資訊設備連線惡意中繼站
- 機關調查發現係同仁至連線設備於**非官方網站**下載影音軟體，於軟體安裝過程中，惡意程式亦一併遭安裝至電腦，導致電腦受駭

遠距辦公與公共 Wi-Fi 主要資安問題

資料被竊取：駭客在未加密的公共 Wi-Fi（例如假冒的熱點）上攔截數據，可竊取帳密、銀行資訊、機敏文件等。

惡意軟體與勒索軟體：透過釣魚郵件或惡意附件，將勒索軟體感染個人設備，進而影響公司內部系統。

弱密碼與帳號洩漏：使用預設或重複密碼，一旦被破解，駭客能輕易入侵公司網路。

不安全的個人裝置：家用路由器未更新、個人裝置未加密、物聯網 (IoT) 設備成跳板，留下安全漏洞。

檔案共用風險：遠端共用文件時，若未遵循加密標準，資料可能外洩。

晶片漏洞：某些 Wi-Fi/藍牙晶片漏洞會被利用，導致密碼與資料被竊取



遠距辦公與公共 Wi-Fi 主要資安問題

資料被竊取：駭客在未加密的公共 Wi-Fi（例如假冒的熱點）上攔截數據，可竊取帳密、銀行資訊、機敏文件等。



遠距辦公與公共 Wi-Fi 主要資安問題

弱密碼與帳號洩漏：使用預設或重複密碼，一旦被破解，駭客能輕易入侵公司網路。





應對與防護建議

強制使用 VPN：在公共 Wi-Fi 上連線公司網路時，使用 VPN 建立加密通道，保護數據傳輸。

確認網站安全性：只瀏覽使用 HTTPS (https://) 的網站，並避免在公共 Wi-Fi 登入銀行或輸入敏感資料。

強化設備安全：更新家用路由器韌體與密碼。保持作業系統、防毒軟體、應用程式最新。關閉不必要的藍牙等連線。

避免使用公用電腦：絕對禁止在公共電腦登入公司系統。

資安教育與政策：定期對員工進行資安培訓，提高警覺，並制定清晰的遠端工作資安政策。

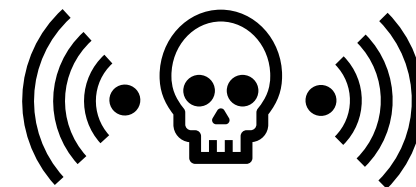
使用安全的通訊工具：選擇有端到端加密 (E2EE) 的雲端通訊軟體。

手機熱點優先：使用手機 4G/5G 熱點比公共 Wi-Fi 更安全。

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





AGENDA

1

常見的網路攻擊態樣

2

辦公室實體與遠距安全

3

保護智慧財產權、**ODF**開放文件應用、資通安全政策宣導

4

社交工程

5

個人資料保護法與實務
應用重點

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。

智慧財產權範例

營業秘密：TGo 會員網站

符合秘密的資訊、具有經濟價值與合理的保密措施三要素。



圖片來源：翻爆

商標：台灣高鐵

台灣高鐵標誌的設計靈感來自飛舞中的旗幟。由輕盈的線條組成，卻充滿旺盛的張力。

專利：外觀設計

車頭的立體弧狀造型，重點在於視覺效果而非技術、功能，由設計專利來保護。

著作權：照片本身

拍攝這張照片。



法律人

教學涉及的四大著作利用行為



重製

影印書籍、下載圖檔、轉貼文章作為講義教材。



公開播出

在課堂上播放音樂CD，輔助解說課程內容。



公開放映

在課堂上播放DVD影片或動畫（須與授課相關）。



公開傳輸

將教材上傳數位平台或透過網路進行遠距教學。

授課合理使用的「關鍵準則」

- ✔ **必要性**：與授課內容有直接相關，非僅為娛樂。
- ✔ **正當性**：已公開發表之著作，且註明出處。
- ✔ **比例性**：影印比例不得傷害著作權人利益（如以影印替代購買）。
- ⚠ **禁忌**：將完整教科書影印或隨意播放整部商業電影。



遠距教學與數位教材資安防護

雲安維運

聯防設備

風險檢測

顧問諮詢

資安學苑



100% 封閉式環境

採取合理技術措施：

- 設置帳號密碼登入機制。
- 防止非選課學生接收課程內容。
- 出版商資源上傳校園平台須注意授權期限。

著作利用「質」與「量」的量化參考

著作種類	合理使用標準 (參考美、港實務)	備註
書籍 / 期刊	單章、單篇或作品總頁數之 10% 為限	以較少者為準
詩 / 短文	詩：250字以內；文章：2500字以內	同作者限1篇
插圖 / 照片	單一作者不超過 5 張；整本畫集不超過 10%	須註明來源
影音 / 動畫	不超過 10% 或 3 分鐘 (音樂 30 秒)	不改變基礎旋律
利用時間	數位教材首次利用後，最多再利用「2年」	超過須重取授權



尊重智慧財產權，共同維護學術與創作環境

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。

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>



國立臺南大學
智慧財產權宣導作業管理系統
INTELLECTUAL PROPERTY RIGHTS OF NUTN

宣導作業最新消息

管理系統開發源起

智財權法令與案例

宣導作業管理系統

宣導作業參考文件

資安事件處理標準程序

智慧財產權宣導網

麗文校園書局南大店

二手書店

智慧財產權宣導最新消息 News

2026/03/19 教育部函轉經濟部智慧財產局加強宣導請各校積極輔導、提醒學生使用正版教科書（含二手書）發函

2026/03/19 教育部函轉經濟部智慧財產局「教師授課著作權錦囊」宣導資料發函

2025/06/18 素養小知識：法律與著作權，歡迎教職員生瀏覽參閱，增進保護著作權認知。（資料來源：中小學數位素養教育資源網）

2025/06/18 為提升教師正確著作權觀念，請各單位協助宣導教師參用經濟部智慧財產局之「教師授課著作權錦囊」。

2025/06/18 請相關行政及系所單位積極輔導、提醒學生使用正版教科書（含二手書）

more ▶

智慧財產權宣導活動訊息 Activities

2026/03/19 114年度智慧財產權教育宣導成果報告

2026/03/19 114年度「AI人工智慧相關著作權」講座簡報

2025/11/05 教師授課著作權錦囊，歡迎教師參考運用。

2025/11/05 114年度「專家服務團智慧財產權講座」活動資訊-經濟部智慧財產局

2025/11/05 114年度「政府機關人員的著作權必修課」宣導說明會

more ▶



什麼是 ODF 文件應用工具？

為引導公務與教育機關落實開放格式，促進跨機關流通而開發之核心工具。

標準化編輯：完全支援編輯與保存標準 ODF 格式。

商用轉檔：支援商用文件格式（如 MS Office）快速轉為 ODF。

範本集與編碼：內建豐富的公務文件範本，並支援 CNS 11643 中文全字庫。

安全合規：工具採開放原始碼機制（MPL v2.0），經嚴格軟體源碼安全掃描。



多系統支援與極致安全防護



跨平台多作業系統支援

全面覆蓋校園常用辦公設備環境：

- **Windows**：提供 32 位元與 64 位元主程式安裝。
- **macOS**：完美支援 Apple Silicon 架構，提供中文語系安裝檔。
- **Linux**：提供 Ubuntu Linux 專屬 DEB 手動安裝包。



開源碼透明性與合規安全

符合公務與學術最高資安合規：

- **開源授權**：遵循 Mozilla Public License v2.0，原始碼安全透明。
- **源碼掃描**：最新 4.0.4 版本提供完整軟體源碼掃描報告。
- **合規使用**：防止惡意軟體後門，確保學術研究與校園文件流通販佈安全。

完善的數位教材與諮詢管道



詳細操作手冊

提供 Windows 4.0 版、
macOS 及 Ubuntu Linux 各平
台專屬安裝與操作說明手冊
(ODT/PDF 雙格式)，降低使
用門檻。



三大核心教材

數位教材一應俱全：包括
Writer 文書進階、Calc 試算
表進階、Impress 簡報進階，
協助同仁迅速由舊工具無痛
轉移。



問題回報與客服

內建 Q&A 回報程式、全台
ODF 小幫手。聯絡信箱
odf@moda.gov.tw，電話
02-7709-4226 竭誠為您解
答疑惑。

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>

爲什麼我們應該使用 開放文件格式 Open Document Format



- 01 支持ODF所代表開放與平權的普世價值
- 02 ODF文書軟體功能非常齊備
保證滿足絕大多數工作需求
- 03 從此不必再煩惱購買文書軟體授權

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>



國立臺南大學資通安全宣導網 ★南大首頁 網站導覽

國立臺南大學資通安全宣導網

國立臺南大學資通安全宣導網 » 國立臺南大學導入資通安全暨個人資料管理規範 » 臺南大學資通安全宣導網

- 115年資通安全暨個人資料管理規範導入顧問輔導服務-教育訓練課程
- 國立臺南大學導入資通安全暨個人資料管理規範 >
- 教育體系資通安全管理規範驗證證書
- 中小學網路素養與認知網
- 資安漏洞警訊公告(國家資通安全研究院)

115年資通安全暨個人資料管理規範導入顧問輔導服務-教育訓練課程👍

(No Title)

資通安全管理法及相關法規命令修正施行(數位發展部主管法規查詢系統)

115年各單位保有資訊資產及個人資料檔案風險評鑑作業說明(登入表單系統填報)

115年各單位保有資訊資產及個人資料檔案清查盤點作業說明

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)	

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。



AGENDA

1

常見的網路攻擊態樣

2

辦公室實體與遠距安全

3

保護智慧財產權、ODF開放文件應用、資通安全政策宣導

4

社交工程

5

個人資料保護法與實務
應用重點

資安事件類別



網通設備疏於更新或使用
弱密碼導致存在資安風險



未即時修補系統漏洞，導
致漏洞遭利用入侵系統



郵件帳號或網站後台設置
弱密碼遭暴力破解，導致
資料外洩



設備與網站資料維護不
當，導致系統受駭或資
料外洩



網站遭DDoS攻擊，導致
無法正常提供網站服務



人員資安意識不足，開
啟惡意郵件或下載夾帶
惡意程式之軟體，導致
設備受駭

2024~2025年需警戒的5大資安風險

非惡意軟體(Malware-free)攻擊



資料來源：2024 iThome CIO大調查，2024年4月

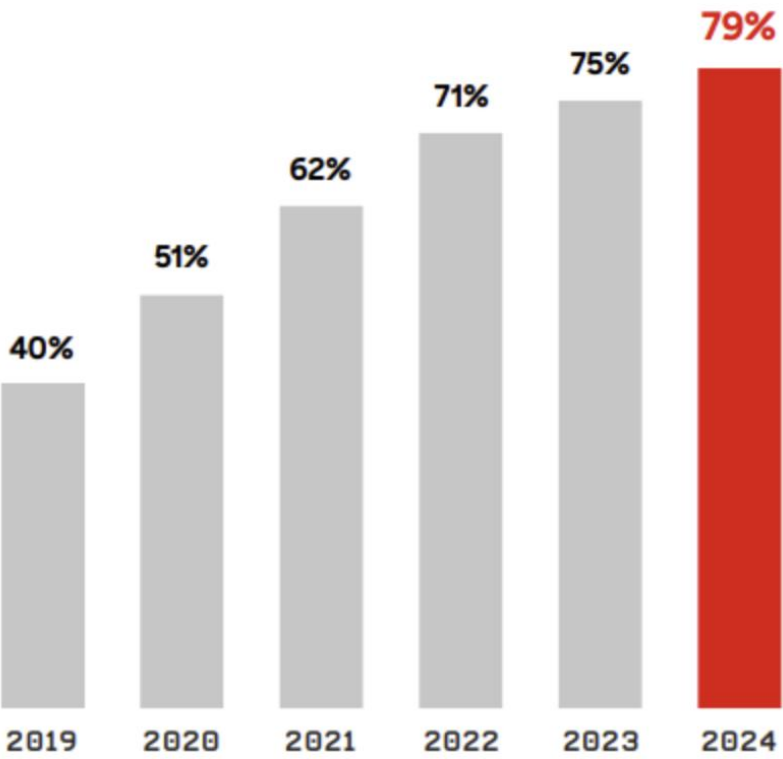


Figure 4. Percentage of detections that were malware-free, 2019-2024

何謂社交工程



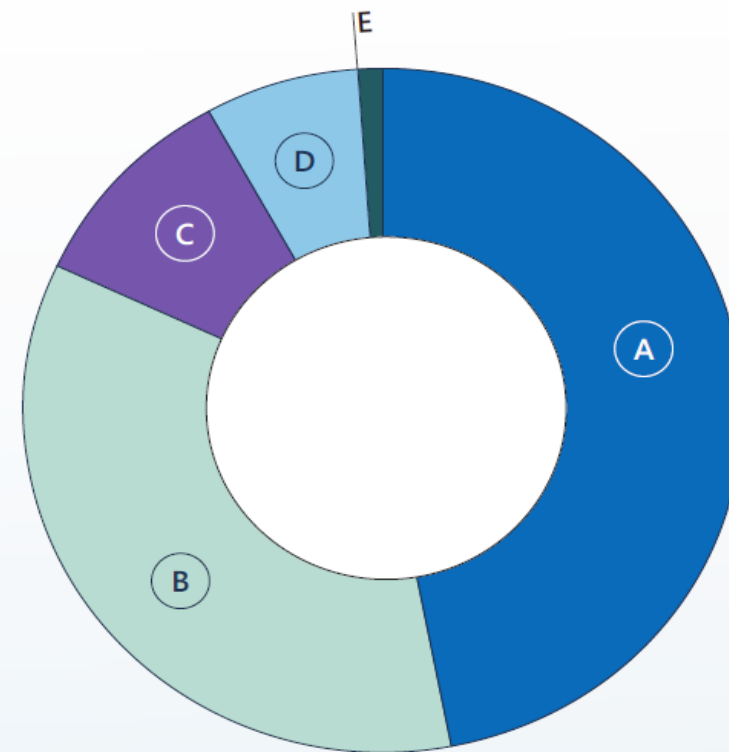
何謂「社交工程攻擊」？

首先讓我們先了解一下

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。

Top initial access methods observed



A. ClickFix	47%
B. Phishing	35%
C. Password spray	10%
D. Drive-by compromise and SEO poisoning	7%
E. Vulnerability	1%

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

社交工程常見手法

網路釣魚

- 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

← Re: 「24小時內生效」您的電話號碼變更...



卡片安全中心
收件者: 卡片安全中心

1月21日 ☆

詐騙又換新方式了，
請大家小心！

變更確認



CTBC BANK
中國信託銀行

您好，

您要求將與您的卡片綁定的主要電話號碼更改為
+886 2 1230 7265，目前正在處理中，以確保安全性。

您的新號碼將在 24 小時內與您的卡片綁定！

如果您確認此變更，則無需採取進一步行動。請忽略此郵件。

如果您想取消此變更，或懷疑有人未經您的同意申請了此變更，請立即採取行動：

取消變更

使用您的電話號碼，您可以：

- 確認您的身份以進行線上訪問。
- 使用您的 Mastercard Gold 授權線上購物。



刪除



回覆



轉寄



移動



更多



雲安維運



聯防設備



風險檢測



顧問諮詢



資安學苑

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

建議：
務必確認網頁名
稱是否正確，以
及網址是否以
https://開頭



Google贊助商廣告

Google 搜尋第一條連結不要馬上點！ 專家指「惡意廣告」已成駭客目標

網路安全軟體公司 Malwarebytes 資深研究總監 Jérôme Segura 表示，近期美國的「惡意廣告」事件增加了 42%，**駭客偽造了幾乎所有類型的品牌相關網站**，並透過 Google 搜尋的贊助商廣告功能，植入惡意連結以進行網路釣魚。

這些被駭客惡意投放的贊助商廣告，不只是會出現在搜尋結果的最上方，還有可能透過廣告聯播網，擴散到其他經常民眾被造訪的主流網站。

機車強制險

全部 購物 圖片 新聞 影片 網頁 地圖 更多

贊助商廣告



cathay-ins.com.tw

<https://www.cathay-ins.com.tw>

國泰機車任意險兩年期方案 - 每天不到10元再享30公里道路救援 ✓

贈送之道路救援為本公司委託合作廠商之加值服務，非屬保險契約之權利與義務。國泰特推機車保單，強制險不賠償的就讓任意險幫你扛...

機車強制險，最高折215元

投保一年期享保費優惠145元 投保二年期保費優惠215元

好市多黑鑽會員獨享優惠

黑鑽卡會員保國泰產險享專屬福利 線上保任意險享87折再抽萬元好禮

贊助商廣告



新安東京海上產物保險

<https://www.tmnewa.com.tw>

機車 強制險 首選【新安】 - 【新安機車強制險】最高現省\$215 ✓

24H網路試算投保，降低接觸風險，不必出門，4步驟快速獲保障！保費享82折專屬優惠，馬上了解

贊助商廣告



msig-mingtai.com.tw

<https://www.msig-mingtai.com.tw> 機車強制險優惠，任意險最高86折

明台機車險線上投保享近86折優惠 | 機車強制險現省，任意險... ✓

人包鐵上路前保障不能少，線上投保超方便，任意險保費最高86折，保障不能等，現在就立即行動！

媒體釣魚

- 幫寵物/小孩投票
- 網購時被要求物流認證
- 各機關催繳簡訊(附短連結)
- 各服務商的服務細節變更通知

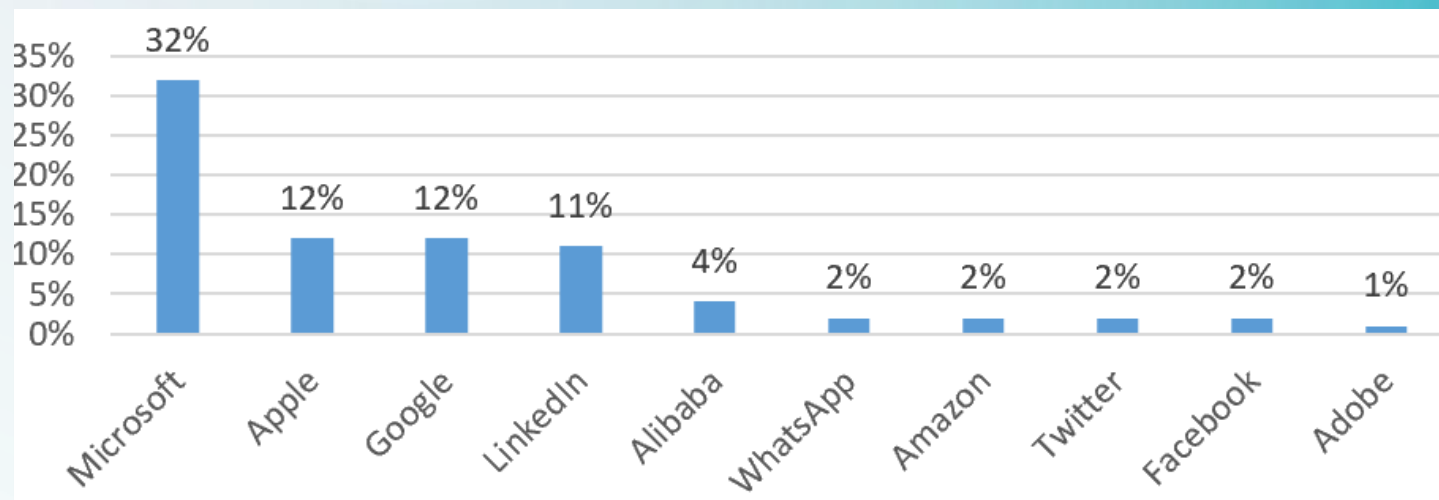


社交工程

品牌釣魚

- 惡意行為者偽裝成知名的品牌，透過電子郵件、網站、社群媒體等方式，誘騙使用者點擊惡意連結、輸入敏感資訊，以竊取個人或企業的資訊。

2024年第4季 品牌釣魚排行



實際案例 - 遠通ETC

你可以先知道：

- (1) 假冒「遠通電收」的簡訊詐騙，輸入資料會盜刷信用卡！
- (2) 當收到結尾有「繳費連結」的簡訊，請務必提高警覺！



台灣事實查核中心
Taiwan FactCheck Center



雲安維運



聯防設備



風險檢測



顧問諮詢



資安學苑

社交工程常見手法

媒體掉落(Media Dropping)

故意掉落實體媒體，更進一步還可以在媒體外部標示單位名稱增加可信度

假托/冒名 (Pretexting)

攻擊者會冒名，以捏造的情境，使目標對象採取某行為或提供敏感資訊

恐嚇軟體 (Scareware)

讓目標對象誤信一些假的事實，如信用卡資料外洩、電腦/手機中毒等，並透過提供補正方法的連結導向惡意網站

CEO 詐騙 (CEO Fraud)

以公司內高階主管名義要求員工採取某行為或提供機密資料

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

水坑攻擊(Watering Hole)

透過觀察確認目標對象(或團體)較常瀏覽的網站，於類似合法網站植入惡意程式，靜待目標上鉤

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

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



釣魚服務平台(Phishing as a Service/PhaaS)

LabHost終於被破獲

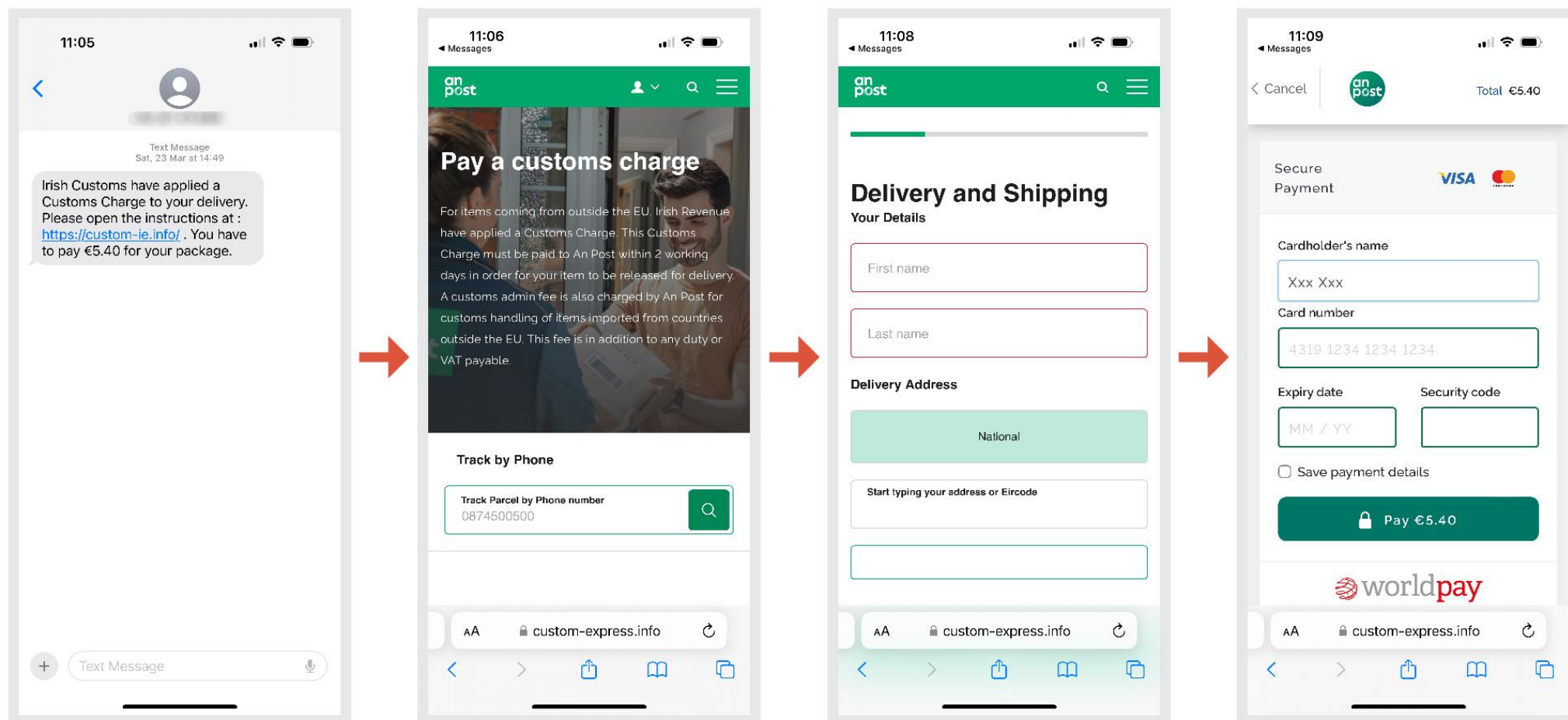
- 針對美加及國際主要銀行，以及其他知名服務設計的網路釣魚頁面。

例如：Spotify 和 DHL

- 高度客製化的網路釣魚頁面，可收集：姓名、住址、電子郵件、出生日期、電話號碼、PIN 碼等
- 容易管理，能為駭客提供多種選擇
- 讓駭客管理他們成功偷到的登入憑證
- 提供熱門的手機簡訊釣魚元件「LabSend」，支援客製化手機簡訊範本，讓駭客輕鬆將網路釣魚頁面發送給受害目標

高級會員月費 **USD 300**

釣魚服務平台(Phishing as a Service/PhaaS)



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

經進一步彙整分析聯防情資資訊，發現近期駭客偽冒資安院，對臺灣學術機構發動針對性社交工程電子郵件攻擊，以「資安攻擊預警」名義，要求收件人執行勒索軟體偵測工具，以因應勒索軟體攻擊活動，惟實則誘騙收件人下載與執行惡意附檔，相關情資已提供各機關聯防監控防護建議。

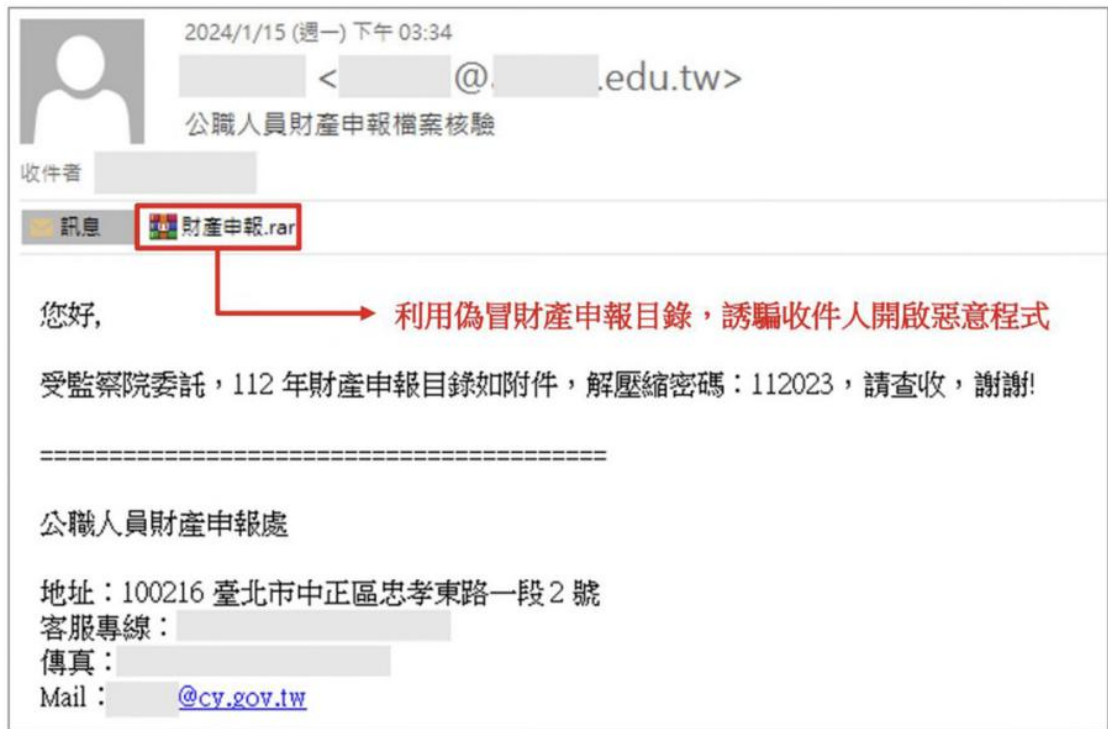
經進一步彙整分析聯防情資資訊，發現近期駭客偽冒財政部名義並以稅務調查為由，對政府機關與台灣企業機構發動社交工程電子郵件攻擊，並針對具敏感資訊存取權限之財務人員，誘導開啟並點擊附檔內含之惡意連結，相關情資已提供各機關聯防監控防護建議。
資通安全網路月報（114年2月）

經進一步彙整分析聯防情資資訊，發現近期駭客偽冒企業之法律部門以侵犯著作權法為由，誘騙收件者點擊郵件內之釣魚連結並填寫表單進行申訴，以達竊取敏感資料目的，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3月）

偽造成業務相關的郵件

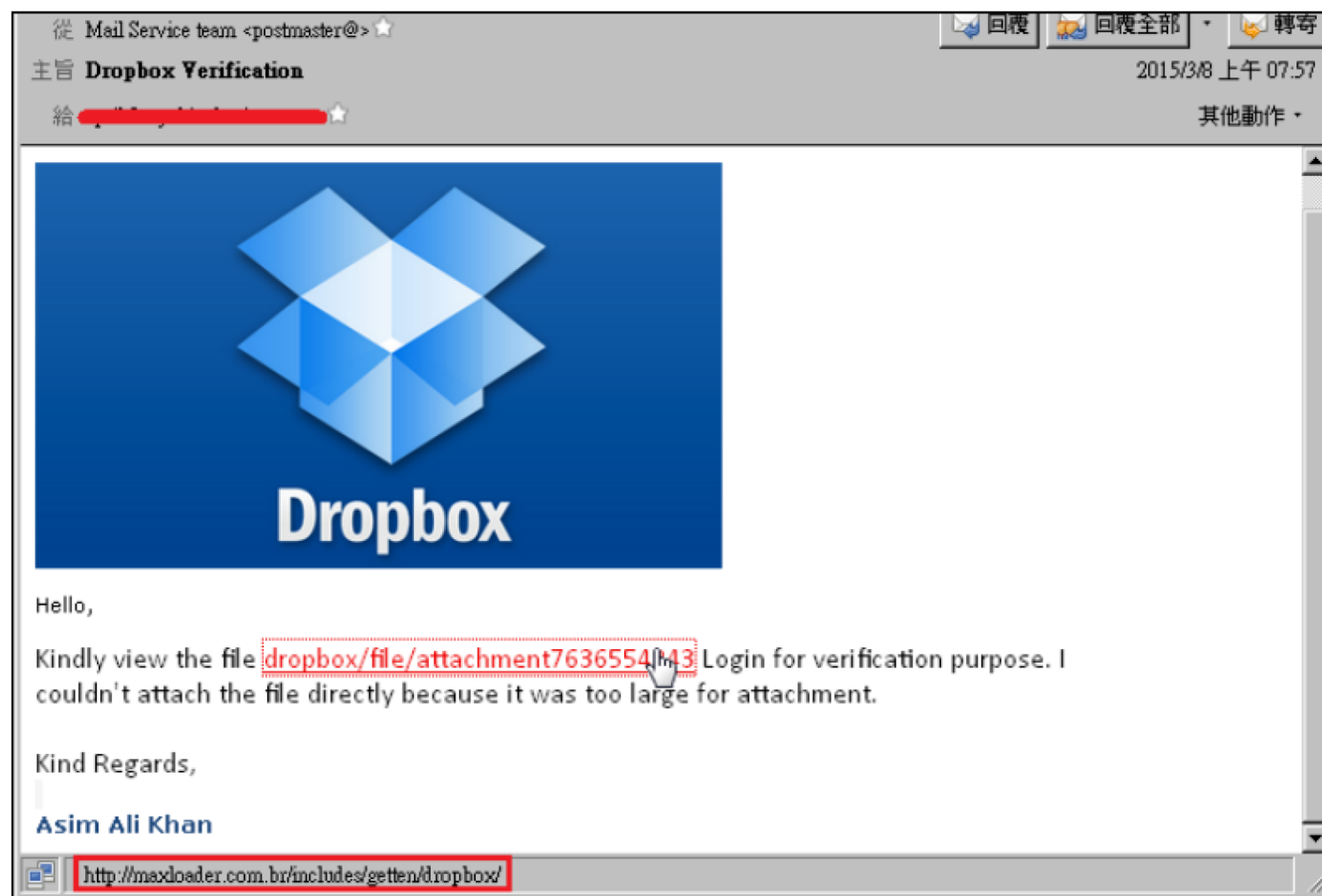
案例一

- 資安院發現駭客利用大學系所人員之電子郵件帳號，偽冒監察院名義，**寄送含惡意附檔之社交工程電子郵件**給政府機關人員
- 信件主旨：公職人員財產申報檔案核驗
- 部分政府機關人員接獲信件後，信以為真，啟惡意附檔後遭植入後門程式

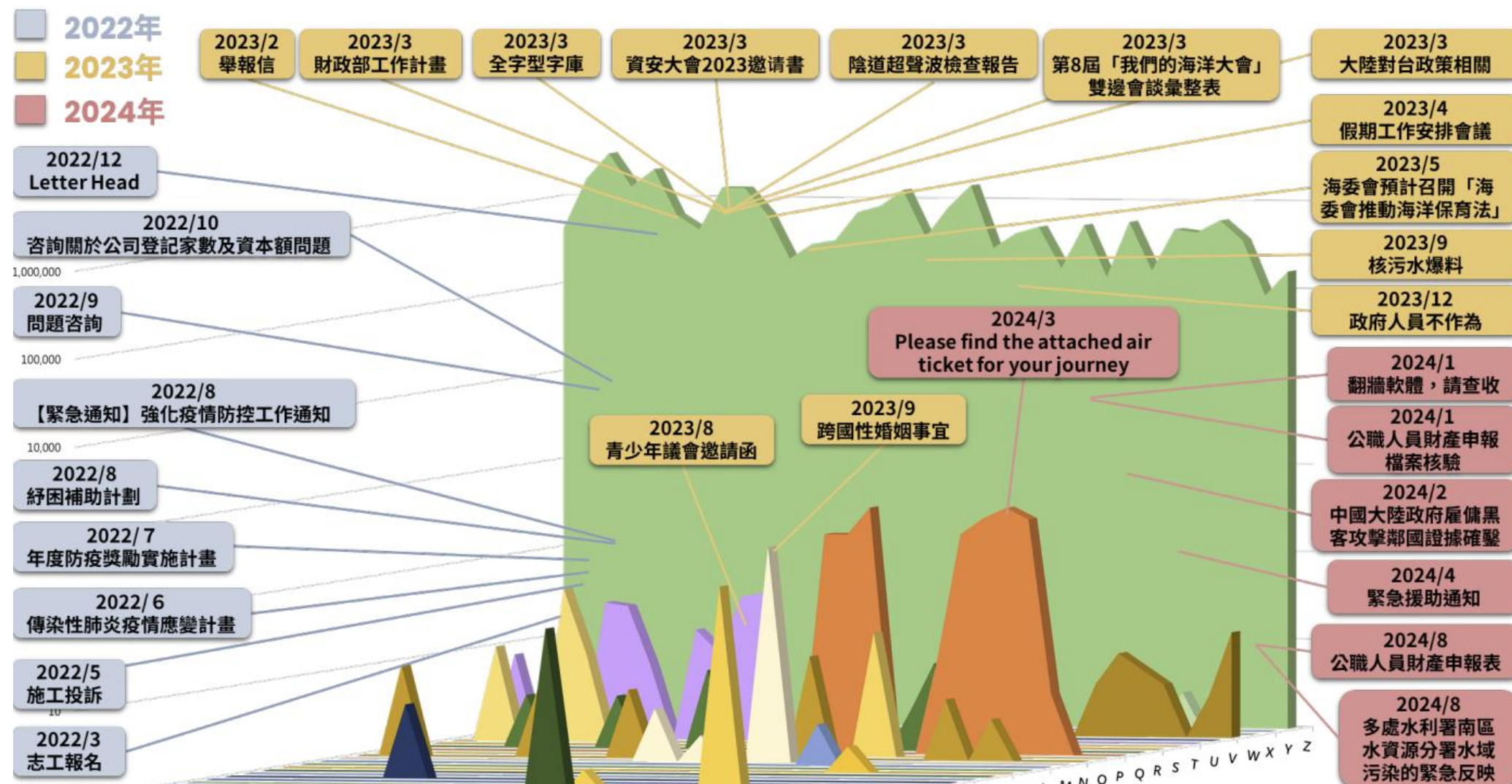


郵件中的惡意連結及惡意附件

看似Dropbox的系統信件，實際上連結指向受感染的網頁



2024年政府領域APT郵件攻擊趨勢



詐騙信件也吹復古風？



就算沒有老花也難以看出!

那只要不開附件也不點擊連結，就安全了...吧？

不見得！

- 有些病毒只要在預覽窗格中看到這封信就能夠感染
 - 有些惡意程式會利用ActiveX功能來執行
- 電子郵件可能是以HTML格式編輯，ActiveX可以透過HTML撰寫，導致電子郵件一經開啟，便自動觸發ActiveX的執行



郵件中的隱藏內容

不易發現的外部連結內容

- 發信者在郵件中，放入不易發現的外部連結內容，例如透明或尺寸極小的外部圖片，郵件軟體為了呈現該圖片，會自動依信件內的指示向外連結該圖片網址。
- 這手法在駭客釣魚信件中會用到，在社交工程演練也會用到！



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
3. 【預設讀信方式】選擇純文字
4. 【封鎖外部圖檔】選擇全部封鎖並勾選內文圖片要封鎖
5. 【與業務無關】請特別注意這類信件，盡量避免開啟

資通安全網路月報(113年1月)

資安署示警公務帳密外洩頻傳 籲勿濫用公務信箱

<近期政策重點>

近來發現部分同仁使用公務信箱註冊於非公務網站，致遭帳密外洩案例，重申公務信箱勿註冊於非公務網站或外部服務，且不可使用相同通行碼，避免外部主機遭駭侵後，相關帳號、密碼及使用者個資等資料都將一起曝險；另使用者電腦系統及軟體亦應定期更新及掃毒，以維資通安全。

找個厲害的平台先幫我看看

惡意檔案檢測服務

Virus Check

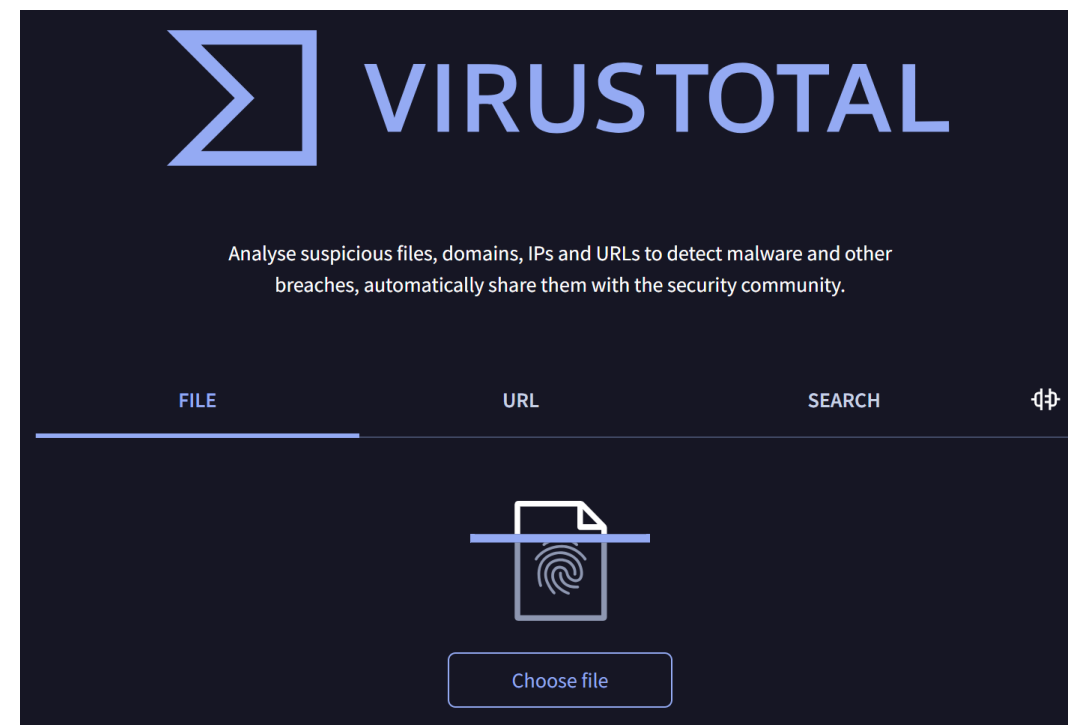
Integrate static and dynamic cybersecurity analyzing skills;

Detect hidden malware in a comprehensive manner



檔案上傳 File Upload

選擇檔案 未選擇任何檔案



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。

純文字瀏覽

非純文字

純文字

Hi [redacted]
如：致IT管理上。

1. 1 / 2 附圖中夾雜使用，此圖為2014年資安大會，由陸院DC24002401
2. 已當地點與時間可，此圖為某市之會議中



File Message Help

🗑️ 📁 📧 🛡️ ⏪ ⏩ ➡️ 🗑️ Share to Teams

[redacted]

From: 黃曉娟 Ellen
To: [redacted]

① You replied to this message on 2014/02/12 09:04.
Use the previous link to change this photo from former

🌐 Translate message to English | Never translate from Chinese (traditional) | Translation preference

Hi [redacted]

如：致IT管理上。

1. 1 / 2 附圖中夾雜使用，此圖為2014年資安大會，由陸院DC24002401

2. 已當地點與時間可，此圖為某市之會議中

防騙停看聽

停

- 安裝防毒軟體，確實更新病毒碼
- 取消信件預覽功能，以純文字模式開啟信件
- 設定過濾垃圾郵件機制

看

- 信件【寄件人】郵件地址。如：**service@mail.tainan.gov.tw**
- 【主旨】或【內容】是否與本身業務相關，是否帶有簡體字或是非熟悉的地區用語
- 移動滑鼠確認連結，附件先右鍵儲存後經掃描再開啟

聽

- 開啟前透過電話或電子郵件向寄件者確認真偽(如：委外廠商聯絡人)
- 詢問機關資訊單位疑似狀況

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

利用Deepfake技術，騙走2億港幣

2億港幣咻咻咻就不見了

報案人為一家跨國公司的香港分行員工，該職員**收到一封據稱是該公司駐英國財務長的電子郵件**，其內容聲稱與公司秘密交易有關。雖然該員工當下曾經有所懷疑，但由於該會議邀請該公司數名財務職員**進行多人視訊會議**，該員工在加入視訊會議後，看到與會成員的影像都是他認識的同事，有著與現實相同的容貌，因此放下先前的疑慮，並依照會議中指示，陸續轉帳15次，將2億港幣轉帳到5個當地的銀行帳戶，等到後續向總部查詢，才知道受騙。



你的朋友不是你的朋友



IBM認證的5個可以降低損失的方法



(1) 進行人員教育訓練

效益最大

- (2) 導入AI及自動化
- (3) 建置SIEM偵測監控系統
- (4) 備妥事件應變計畫
- (5) 進行檔案資料加密及備份

駭客不駭電腦，他們駭的是「人」

社交工程防禦與資安意識建立

臺南大學資訊網 – 社交工程宣導

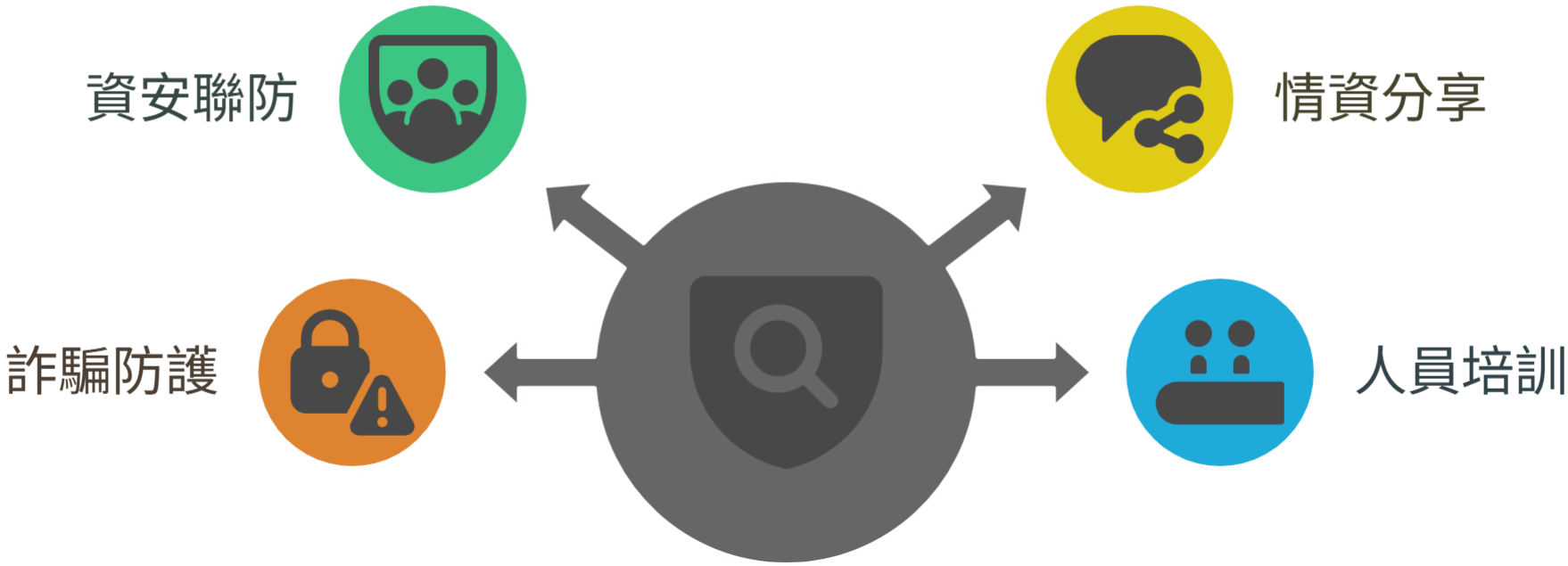


網址：<https://www.nutn.edu.tw/cc/emailse/about.html>

»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。

結語-養成資安警覺心

提升資安敏感度





AGENDA

1 常見的網路攻擊態樣

2 辦公室實體與遠距安全

3 保護智慧財產權、ODF開放文件應用、資通安全政策宣導

4 社交工程

5 個人資料保護法與實務應用重點

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

(114.11.11修法公布)

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



個資保護簡介

1. 蒐集處理利用應有**特定目的**，並應與蒐集之目的具有正當合理之關聯。
2. 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。
3. 告知義務與通知義務
4. 維護資料正確性
5. 刪除資料義務
6. 公開義務
7. 不適用情況



什麼是個人資料

個人資料定義§2、§6

- 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

一般資料

- 病歷
- 醫療
- 基因
- 性生活
- 健康檢查
- 犯罪前科

特種資料

- 其他得以直接或間接方式識別該個人之資訊

其他



個人資料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

蒐集

處理

利用

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

蒐集的告知義務

直接蒐集§8、間接蒐集§9

機關名稱

當事人之權利及
行使方式

蒐集目的

得選擇性提供時，不提供
將對其權益造成之影響

個人資料之類別

資料利用之期間、地區、
對象及方式

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. 與您的人際網
10. 您的照片、金
11. 基於我們的登
12. 行銷及通訊資
13. 使用及交易

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，財政部所屬分局、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、保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

蒐集 利用

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。

利用

個人資料的合法利用

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

利用

個人資料的合法利用

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…」。

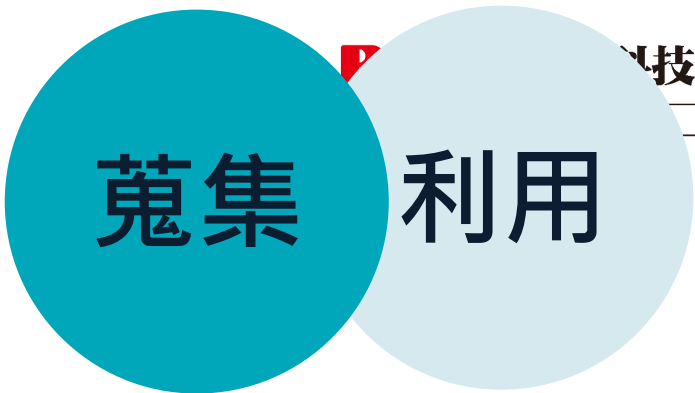
查警察機關溯源追查供毒網絡，固屬維護國家安全與增進公共利益之目的，然本件「社會安全網－關懷 e 起來通報平台」所蒐集之施用毒品等兒少個案資料，原係為協助兒少後續就醫、保護、安置或為其他必要處置，如將相關資料做上述目的外之利用，使原應受保護、關懷之兒童少年成為警察機關之關注對象，除可能妨礙兒少權益保障之原始目的達成外，亦與個人資料之利用應符合誠實信用方法之原則有間，尚難認符合個資法第 5 條之規定。

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。

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	身分證字號號碼
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
身分證字號查地址	專案價	5-7天	身分證字號	目前戶籍地及居住地
身分證字號查姓名	專案價	5-7天	身分證字號	現在姓名
身分證字號查電話	專案價	5-7天	身分證字號	名下市內電話或手機號碼
身分證字號查照片	專案價	5-7天	身分證字號	個人照片
身分證字號查名下車輛	專案價	5-7天	身分證字號	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

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护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护作業要點第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

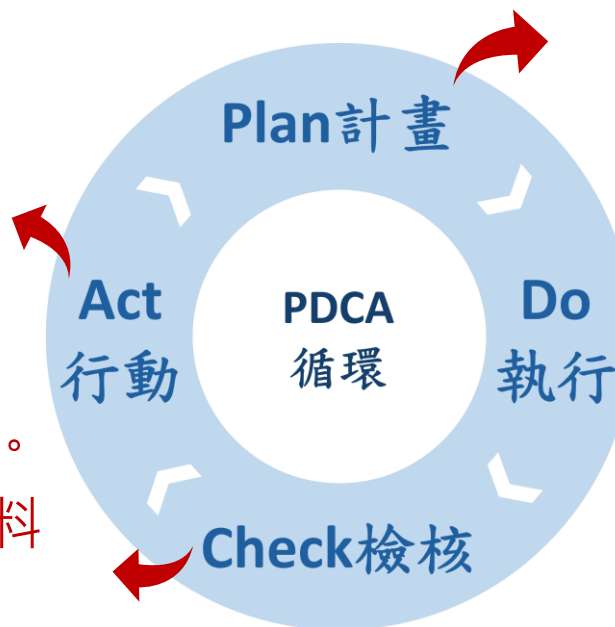
適當之安全維護措施

措施種類(細則§12)

- 組織上措施
- 技術上措施

十一、個人資料安全維護之整體持續改善。

九、資料安全稽核機制。
十、使用紀錄、軌跡資料及證據保存。



- 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。

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



個人資料檔案清查盤點系統



您好,歡迎使用

回列表

說明文件

登出系統

名稱 >

目的 >

蒐集 >

處理 >

利用 >

保存 >

銷毀 >

揭露 >

重要性

才知道如何分配保護資源--個資風險評鑑範例

名稱	個資類型		風險評估機制					風險管理機制		
	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



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。

系統更新通告

因系統更新作業，
會員贈點活動、基本點發放及
相關折抵活動，今日**全數暫停**。

造成不便 敬請見諒

貼心提示

會員系統已全面升級，
為保障您的交易安全，
請更新密碼。

Breeze
REWARDS

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
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公司接獲教育部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全管理，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!!

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。

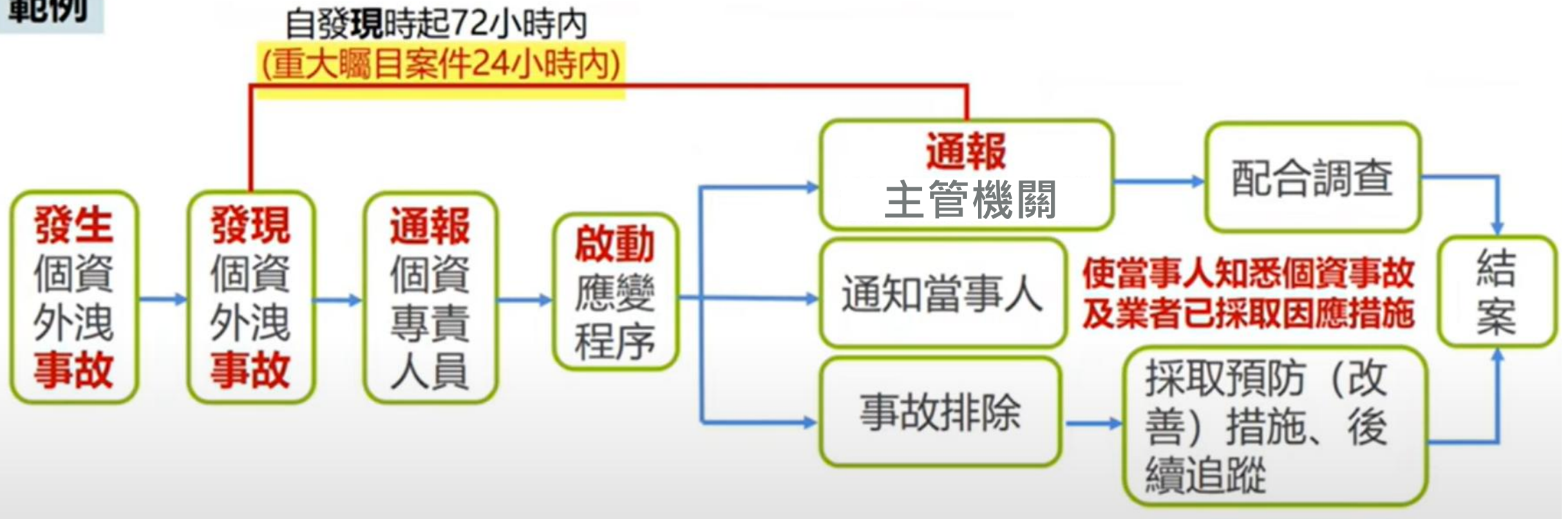
政策目標

- 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)

範例



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>

國立臺南大學個人資料保護宣導網

★南大首頁

📍網站導覽



南大個資管理規範驗證

各單位保有個人資料檔案判斷作業流程

臺南大學個人資料保護宣導教育訓練

國立臺南大學個人資料保護宣導網 » 個人資料保護法施行

國立臺南大學個人資料保護管理政策

國立臺南大學各單位個人資料利用之期間、地區、對象及方式

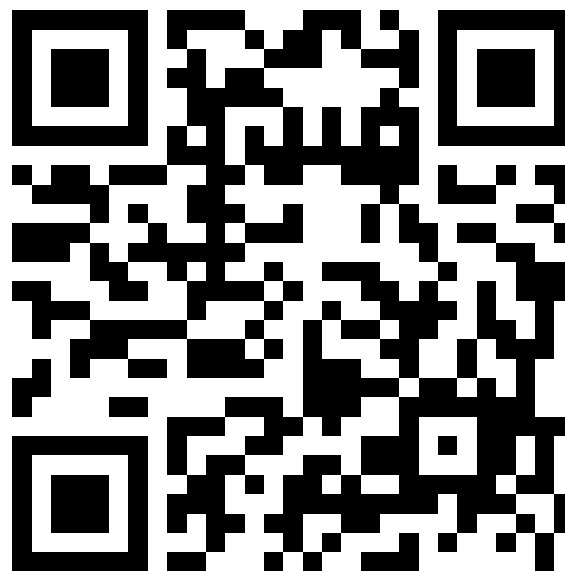
教育部函：請各大專校院加強宣導教職員工及學生個人資料保護觀念，請查照辦理。114年6月20日
臺教資通字第1140065023號函



問題與討論



課後評量



<https://forms.gle/FF3t9MwUG7wobooL6>



- 離你最近的資安專家 -

Thank you

FOR YOUR ATTENTION

Get in touch:



雲安維運

聯防設備

風險檢測

顧問諮詢

資安學苑