資安星際指南

資安基礎概論

前言與簡介

回顧過往，臺灣企業的資安事故頻傳。研究指出 2023 上半年亞太區共偵測 4,000 億次惡意威脅，其中針對臺灣的攻擊就達到 2,200 億次，佔比高達 55%。根據臺灣證券交易所與證券櫃檯買賣中心所揭露的資訊，2023 年就有 23 起遭網路攻擊的重大資安事件。

這些數據其實僅是臺灣企業資安問題的冰山一角，眞實受害範圍可能更廣泛。網路犯罪並不只針對大型電子科技業，事實上，去年有更多攻擊是針對防禦力較弱的中小企業而來。

「從大處著眼，小處著手」，面對資安問題，需要企業管理層與每一位員工抱持嚴謹的態度面對，逐步將資安防護落實於日常中。

國家資通安全研究院與中小企業、非營利組織共同站在資安風險的最前線，協助大家面對與解決各種資安挑戰。

本資安防護實務手冊希望提供讀者資訊安全的基本概念，配合計畫中的其他教育訓練或輔導，提高企業與每一位組織成員對資安的重視和了解。

透過認識資訊安全對企業及社會的重要性，以及保護組織資訊資產免受威脅和風險影響的方法，讀者將能具備識別與應對常見資安威脅的基本能力。

我們期望這本手冊能成爲您在資安防護道路上的堅實夥伴，共同打造更安全的數位環境，促進企業與社會的共同繁榮與發展。

國家資通安全研究院
National Institute of Cyber Security

目　錄

Tips!

時事連結｜
連結實例新聞
瞭解資安事件

資安案例｜
改寫實際實例
了解資安情境

小註解｜
深入瞭解資安
概念與知識

第一章

資安基本概念

說到資安，您腦中會冒出什麼？是覺得這應該是公司和組織中資訊同仁的業務，與我沒有半點關聯，還是認爲我的電腦、檔案都有好好用密碼保護鎖好，因此相當安全呢？

現在，是時候重新檢視和調整我們對資安的概念，更新自己身爲組織員工應盡的保護義務，成爲了解資安、守護資安的一員。

| 概念 01 |

資安威脅拉警報！從趨勢看駭客手法

報導指出，社交工程及勒索軟體連續兩年都是資安的前兩大威脅。以下將從近年之全球資安威脅與眞實案例出發，歸納出下列四大資安威脅趨勢，顯見現今資安問題的複雜多變，值得企業與組織謹愼應對。

威脅一、網路釣魚為主要攻擊模式

- 隨著人工智慧 (AI) 與新興技術的出現，社交工程 (Social Engineering) 攻擊案例顯著增長，其中網路釣魚仍是最主要的攻擊方式

威脅二、駭客攻擊力道加大

- 國際市場研究機構 Gartner 預測，2025 年全球 45% 組織將遭受軟體供應鏈攻擊 (Software Supply Chain Attack)
- 2023 年軟體供應鏈攻擊，是過去 4 年總和的 2 倍

威脅三、電子通訊設備漏洞層出不窮

- 某國際知名科技服務供應商遭攻擊約 4 萬台設備遭感染
- 殭屍網路 Gafgyt 針對寬頻連網設備供應商的電信網路漏洞進行數千次攻擊

威脅四、勒索軟體技術多樣化

- 勒索軟體橫跨 Windows、Linux 及 macOS 等不同電腦作業系統進行攻擊
- 軟體公司 Veeam 指出 93% 以上的攻擊以備份主機爲目標

什麼是社交工程？

指透過人際互動和操弄來達到詐騙目的的手法。例如：簡訊 /Email 釣魚訊息、要求點擊不明連結等。

深入剖析資安議題

資安領域涵蓋面向多元且複雜性高，許多有意強化資安防護的中小企業與非營利組織不知從何著手改善。比起大型企業，中小企業與非營利組織還更可能陷入缺乏資安預算、資安人力不足的困境，讓增強組織資安防護的過程更加艱辛。

國家資通安全研究院因應各方對資安的需求，推出 NICS 臺灣資安計畫，上至資安政策，下至資安認知，以簡潔易懂的方式引導大家從最基本的層面做起，**例如：個人資料的保護、電子郵件與網路使用安全、委外安全管理。**期望此手冊能帶領各中小企業與非營利組織盤點現有資安措施的不足，進一步加強不足處，並歡迎各方與資安院交流。

資安議題與範疇

資安政策	資訊安全管理系統 ISMS ISO 27001	個人資料保護	法規遵循	資安政策規劃	資安稽核	
資安管理			業務持續運作管理	委外安全管理		
事故處理	惡意程式檢測	數位鑑識		備份與救援	災難復原	
軟體安全&安全檢測	資安健檢	安全系統發展生命週期 SSDLC	源碼檢測	弱點掃描	滲透測試	應用程式防火牆	網站安全 行動裝置安全 物聯網安全
	安全程式碼撰寫					
系統與網路安全	防毒/防火牆	電子郵件安全	網路使用安全	DDoS防護	實體安全	
	資訊資產管理	安全網路架構規劃	網路存取權控制	無線網路安全	IDS/IPS	
資安認知	職前教育訓練	資安意識宣導	社交工程演練	弱密碼管理	人力資源安全	

| 概念 03 |

改善資安：從三大目標談起

若想深入瞭解資安，可從簡稱**「CIA 三要素」**的「資安三要素」著手，這是設計和實施資安措施時可參考並遵守的基本原則。

機密性 Confidentiality

確保只有經過授權的使用者（或軟體系統）可以取得資料與數據，以避免資料外洩或遭利用等風險

- **可能風險：**會員個資、捐款紀錄、顧客訂單資訊外洩
- **解決方式：**資料加密政策、設定權限和身分驗證機制

完整性 Integrity

防止資訊被竄改或破壞，確保資訊的正確性

- **可能風險：**商品價格與銷售資料遭到竄改、網站遭惡意竄改導致訪客被導向釣魚網站
- **解決方式：**監控數據的變化、實施存取控制

可用性 Availability

防止系統故障或遭到人為破壞，使服務受到影響，並確保資訊可被妥善處理及使用

- **可能風險：**遭受網路攻擊，導致網站無法運作
- **解決方式：**維護硬體設備、定期升級作業系統與備份

| 概念 04 |

中小企業與非營利組織面臨的資安風險

網路攻擊、資安事件不再只是大企業需面對的問題，中小企業與非營利組織也須提高警覺，保護好客戶與會員權益。

中小企業面臨的風險

2021 年的研究數據顯示，臺灣 6 成中小企業表示，過去一年曾遭受網路攻擊。其中佔比最高的威脅類型為惡意軟體（84%），其次網路釣魚攻擊（74%），阻斷服務攻擊則居第三位（46%）。

同份研究數據中，在遭受攻擊後有近 7 成中小企業表示遺失客戶資訊、5 成損失敏感商業資料，重要資訊不幸落入惡意行為者手中。

時事連結 資料來源：資安人

超過六成被駭
台灣中小企業遺失客戶數據修復是大挑戰

非營利組織面臨的風險

駭客利用漏洞駭入組織資料庫，竊取捐款人或會員個資，並進行信用卡盜刷及電話和 ATM 轉帳詐騙。後續負面影響包含：公益形象受挫、組織營運能力備受質疑，甚至導致受害者不滿而退出會員。

在駭客技術日新月異的當今，資安防護不同於以往「滴水不漏」的觀念，而是學習降低風險及提升資安韌性，確保在遭遇駭侵的當下可立即反應、即時止損。

| 概念 05 |

上市上櫃公司資訊安全管控指引

爲了避免網路攻擊造成市場重大影響，臺灣證券交易所發佈指引，要求上市上櫃公司配置適當人力及設備進行資安管理。如參考大型企業在資安防禦上的層層分工，共同建立堅實的防護網，中小企業與非營利組織也能從中仿效與學習，使團隊成員間更充分了解各自的角色與責任，在建立資安過程中，沒有人能置身事外。

領導人與管理階層：設立目標與擬定規範

在政策制定與管理方面，管理者可以透過 top-down 的方式，先設立目標與進行風險評估，再擬定各項作業規範及標準；並定期執行內部資安稽核，爲資安防禦立下良好的基礎。`

如果您是組織管理者，可以採取以下措施

- ☐ 成立資安推動小組與制定資安目標
- ☐ 設立資安專責人員
- ☐ 訂定人員裝置使用管理規範
- ☐ 訂定資訊作業委外安全管理程序
- ☐ 定時進行內部資安稽核
- ☐ 模擬遇到資安危機時，如何維持業務運作
- ☐ 設置備份機制及備援計畫
- ☐ 遵守相關資安法令及契約要求
- ☐ 盤點資通系統，並進行風險評估
- ☐ 訂定資安事件應變處置及通報作業程序

人資跨部門合作：資通安全教育訓練

當管理層設定資安相應規範、標準作業流程與稽核機制後，人資應和技術人員合作，安排定期的資安教育訓練、無預警的社交工程演練，模擬最眞實的網路攻擊，確保員工面對不同攻擊能隨時保有警覺性。管理重要數據也是不可忽視的細節，組織平時就應維持標準作業程序，培養人員隨時檢查的好習慣。

如果您是組織內的人資，以下是可以參考的做法

- ☐ 無預警但定期的資訊安全教育訓練、電子郵件社交工程演練
- ☐ 結合資料管理內訓課程，宣導資安意識
- ☐ 製作員工演練結果報告，並向管理層匯報
- ☐ 靈活結合組織績效考核與資安演練、課程

資安人員：技術層面維護

在防禦網路攻擊時，當然少不了資安專責人員的參與，人員能透過開發與維護系統，從技術面支援與確保組織系統安全無虞。

如果您是組織內部的資安人員，以下是需要您技術支援的事項

- ☐ 開發資通系統時，納入資安要求並維護需求規格
- ☐ 定期進行系統安全性檢測並修補弱點
- ☐ 建立偵測與管理資訊安全威脅的機制
- ☐ 資訊安全防護與實體安全控管

| 概念 06 |

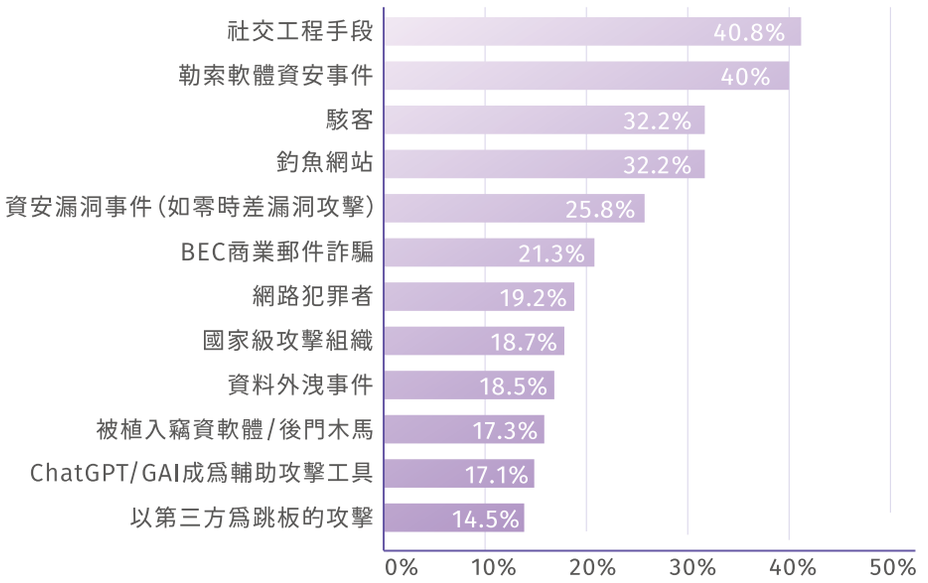
從案例看未來的資安風險

不只高科技與電子製造業，藥局、汽車、觀光、塑膠等傳統製造與服務業也承受著資安風險。2023 年，遭受網路攻擊發布重大訊息的上市櫃公司便高達 17 家。加上地緣政治下資訊戰加劇、疫情後遠距辦公與 AI 崛起等趨勢，資安勢必面臨更多挑戰。

2024 年調查：企業最需警戒的資安風險

- 《iThome 電腦報周刊》調查 422 家大型企業及知名企業 IT 主管對 25 項資安風險的評估，社交工程和勒索軟體與病毒連續兩年名列前兩大威脅
- 第 3 至第 6 名依序是駭客、釣魚網站、資安漏洞以及商業郵件詐騙，而 ChatGPT 與生成式 AI 帶來的風險也不容小覷

未來一年 12 大資安風險 (1)



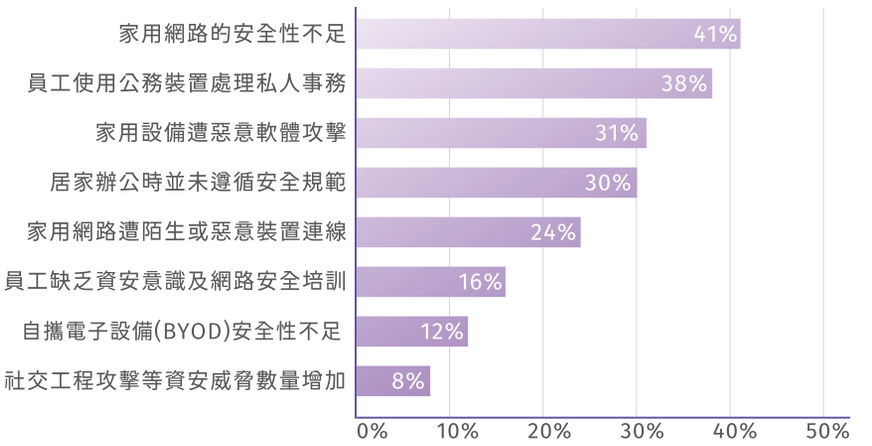
2023 年調查：疫情下遠距工作的新危機

網路安全公司 Fortinet 在《2023 年隨處辦公資安洞察報告》中，對全球及臺灣 570 位資安主管進行調查，結果發現多數企業皆有因採行遠距辦公，而招致資料外洩的經驗，顯示企業仍須加速提升內部資安防禦能力。

遠端辦公的潛在資安風險

- 家用網路及遠端連線的安全性不足，且現階段難以將內部安全架構擴及至外部網路環境，可能招致惡意軟體攻擊
- 員工使用公務裝置處理私人事務
- 居家辦公時並未遵循資訊安全規範
- 家用網路遭陌生或惡意裝置連線

企業認為「隨處辦公」帶來的最大資安風險 (2)



Adapted from

(1) Fortinet® 最新調查：隨處辦公已成職場新主流， 逾六成企業曾因採行遠距工作模式而發生資料外洩

(2) Fortinet®《2023 年隨處辦公資安洞察報告》 (2023 Work-from-Anywhere Global Study)

時事連結 資料來源：Fortinet

2024 企業最需警戒的資安風險

Fortinet：逾六成企業曾因採行遠距工作模式而發生資料外洩

2022 調查：中小企業輕忽資安風險

- 美國媒體《CNBC》2022 年調查發現，只有 5% 中小企業管理者將網路安全視爲最大威脅，企業規模與重視資安程度似乎呈正相關
- 由於大公司越來越重視資安，且攻擊大公司較易被調查單位盯上，駭客紛紛轉而將目標放在中小企業
- 中小企業常成爲「供應鏈攻擊」中最一開始的破口，造成難以想像的財務與品牌衝擊
  - 高達 60% 中小企業會在被攻擊後的半年內宣告停業
  - 55% 消費者表示，不會繼續使用曾受網路攻擊品牌

防備重點

所有企業最大的挑戰是在管控自身安全的同時，也能夠確保供應商的網路安全等級，避免淪爲駭客間接攻擊的目標。

什麼是供應鏈攻擊？

供應鏈攻擊通常是指駭客從一些中小公司的漏洞開始鑽入，進而造成大規模擴散，或透過入侵軟體開發商來滲透。許多中小企業在供應鏈中扮演重要一環，賣給大公司的商品可能很難替代，一但遭遇駭客攻擊，有可能會連帶導致供應鏈中斷。

2021 年資安事件：非營利組織大規模個資外洩

- 盤點非營利組織常使用的資訊服務，其功能包含捐款管理、線上金流整合以及客戶關係管理等。曾經有資訊廠商同時服務多個非營利組織，卻遭駭客攻擊導致大規模個資外洩
- 建議可採取的資安強化措施 ： 限定 IP 位址登入、身分雙重驗證、重要資料加密、建立即時監控系統以偵測異常網路活動等

2016 年資安事件：鎖定政府及非營利組織的多段式攻擊

- 攻擊活動中發現名爲 Trochilus（「蜂鳥」之意）的遠端存取木馬程式 （RAT），是惡意軟體的一種
- 部分木馬程式能避開防毒軟體的偵測，並潛伏在受駭裝置中，在人員不知情的狀況下操作多項功能，並藉此存取重要資料

時事連結 資料來源：iThome

Arbor Networks 發現鎖定亞洲幾國政府及 NGO 組織的多段式攻擊活動

什麼是木馬程式？

這個詞源自於經典的特洛伊戰爭故事，描述一群希臘士兵藏在巨大木馬趁敵方不注意時進攻特洛伊城。在電腦世界裡，木馬是種惡意軟體，透過僞裝成無害軟體，從電子郵件連結或埋藏在惡意網頁中，偷偷安裝在電腦上。

| 概念 07 |

駭客新目標：中小企業

經濟部《2023 年中小企業白皮書》指出，臺灣中小企業已佔全體企業的 98%。儘管大公司的受到網路攻擊次數仍持續增加，針對中小企業的攻擊卻也成長了 13%。顯示數量龐大的中小企業，儼然已成爲駭客的新下手目標。

時事連結 資料來源：Tech Orange

中小企業成駭客新目標！
盤點企業必備的資安防護 3 大基本觀

有鑒於此，中小企業應隨時做好維護資安的準備，以下提供三個企業在資安維護上必備的基本觀念：

1. **養成良好的網路使用習慣**
   如：建立複雜的密碼、將軟體更新至最新版本、遠端使用者及具管理權限的用戶應採取多因子驗證（MFA）
2. **定時進行員工訓練**
   - 舉辦內部社交工程演練，培養人員辨別錯假的能力，以及謹慎行動的習慣
   - 定期舉行模擬演練，以即時因應異常網路行爲
3. **隨時做好應對措施**
   如：制定攻擊發生時的應對策略、定期備份資料和檔案

多因子驗證 (MFA)

是一種要求使用者除了輸入密碼以外，還要輸入額外的身分識別資訊的多步驟登入程序，爲登入流程增加多一層保障。

第二章

資安的風險與威脅

具備基本資安概念後，本節將進一步說明資安在不同層面上，可能面臨的風險與威脅。這八大層面包括：

層面一：資料安全

資料安全指的是「保護資料免於未經授權的閱覽、使用、洩漏、破壞或修改等行爲」。爲落實資料安全，企業或組織可以透過各種技術、措施或安全系統的輔助達成目標。常見的方式包含透過密碼加密和使用者驗證，但就算都做到，仍有許多問題需克服，例如：

狀況一：資訊設備損壞

電子設備有其使用壽命，設備損壞將導致資料無法讀取，是最直接導致資料遺失的原因之一。

狀況二：人員疏失

人員使用電腦軟體或文件時造成的疏失也屢見不鮮。除了教育使用者在操作時應更加謹慎小心，公司或組織也應定期舉辦員工教育訓練，宣導正確的操作及執行流程。

時事連結

資料來源：中央社

2.5 萬筆學習歷程檔案遺失
教部：將補助教師輔導學生重製

資料來源：報導者

「我的愛心被駭客利用了！」
個資外洩風暴下，公益團體的重建信任之路

狀況三：資料外洩

在警政署 165 全民防騙的官網上，皆有公布歷年之「高風險賣場」名單，其中 2022 年的名單上更不乏許多非營利組織。一旦捐款人的資料外洩，不單會造成財務上的損失，也將重創公益團體及捐款人之間的信任關係。

狀況四：勒索軟體

勒索軟體（Ransomware）是種可以破壞使用者存取權限，同時向受害者要求贖金，並使公司內部系統無法正常運作的惡意程式。勒索病毒攻擊通常從惡意電子郵件開始，其中又可分爲「非加密型勒索軟體」及「加密型勒索軟體」兩種。不要隨意點擊來路不明或未經確認的連結，是防範勒索軟體的首要工作。

資安案例

連假是集體出遊的好日子，但在端午連假前夕，綠島船班的電子商務網站遭駭客入侵並勒索，導致網站無法運作，遺失訂票紀錄。

延伸閱讀

國家資通安全研究院——勒索軟體防護

不同類型的勒索軟體

- ◇ 非加密型勒索軟體：將受駭者的資訊設備鎖起來、不讓其登入；但取回存取權後，檔案均能保留。
- ◇ 加密型勒索軟體：加密受駭者硬碟上的檔案，破壞受駭者對資料的存取權。

資料安全的防護方式

隨著駭客的攻擊手段愈趨多元，企業與組織也須致力於提升內部人員的資安防護意識，並定期備份資料，確保各裝置處於受到安全防護狀態，以有效降低受駭時的損失。

防護資料安全的方法有很多，建議從以下著手

- ☐ 定期備份檔案，備份頻率視資料重要性而定
- ☐ 確保軟體隨時更新至最新版本，以修補軟體漏洞
- ☐ 謹慎開啟郵件，不點擊不明連結或安裝陌生程式
- ☐ 安裝防毒軟體，隔離已知病毒

在現今數位化的時代中，大量的電子資料已是企業與組織的重要資產，故資料保護比以往來得更加重要。舉例而言，過去惡名昭彰的 WannaCry 勒索病毒，至今仍持續衍生出新的變種，不斷威脅著全球網路安全。

根據統計，該病毒於全球造成高達 40 億美元的商業損失。不僅導致重要資料落入駭客手中，更造成產能下降、生產效率降低、資料復原成本上升等種種問題，讓許多組織深感頭痛。

小知識：備份資料的「3–2–1 原則」

備份資料很重要，但應該如何備份資料呢？
「3-2-1 原則」是您可以採取的備份方法之一！

3 是重要資料至少備份 3 份
2 使用 2 種不同的方式進行備份，如外接硬碟、USB
1 將其中 1 份備份存放異地

層面二：社交工程

社交工程是攻擊者利用人性的弱點，誘騙他人洩漏機密資訊或執行特定動作的攻擊手法。攻擊者在透過社交工程騙取被害人信任後，可能進一步發動其他攻擊行為，例如：安裝惡意程式、關閉電腦的安全防護模式、誘騙被害人至 ATM 進行轉帳等。

社交工程的常見攻擊方式如下：

1. 利用電話佯裝客服人員，騙取帳號及其他機密資料
2. 偽裝委外廠商之維護人員或上級單位，乘機騙取帳號及密碼
3. 利用電子郵件誘騙使用者登入偽裝之網站，以騙取帳號及密碼，如網路釣魚
4. 利用電子郵件誘騙使用者開啟檔案、圖片，以植入惡意程式、暗中收集機密資料
5. 以提供工具、偽裝的檔案，誘騙使用者下載，乘機植入惡意程式並暗中收集資料
6. 利用 LINE、Messenger 偽裝成親友降低受害者的警戒心，並傳送帶有惡意連結的訊息

資安案例

上市櫃公司遭駭客冒名，發送虛假電子郵件通知客戶更改收款帳戶。通常詐騙能成功，代表駭客已掌握雙方款項交易行為，例如入侵電子郵件、閱讀公司信件，須特別留意電子郵件防護。

社交工程的基本防護認知

不同於駭入技術，往往需具備專業的資訊技巧與背景，社交工程攻擊僅透過對話或訊息往來，就可能成功到騙取受害者的資料，也是一般人更常遭遇的問題。因此，除了對來路不明的連結及程式保持警惕外，也應提升自身的基本防護認知。

以下是面對社交工程時，可以做到的防範措施：

1. 隨時提高警覺，在未經查證的情況下不輕信他人
2. 在尚未確認對方身分之前，不應提供資料給對方
3. 不開啟來路不明的電子郵件及附加檔案
4. 不點擊連結及登入未經確認的網站
5. 不下載非法軟體及檔案
6. 遇到疑似攻擊事件時應向有關單位通報，如單位主管、資安單位、警方等

溫馨提醒 收到類似的詐騙信息時，除了要再三小心，也千萬別急著轉載，避免從受害者變成加害人！

其他社交工程的形式

社交工程的攻擊手法五花八門，除了常見的電子郵件之外，還會利用通訊軟體、手機簡訊、社群網站等各種渠道進行詐騙。

時事連結 資料來源：衛生福利部

不明簡訊「衛福部提供確診者補助金」爲詐騙訊息

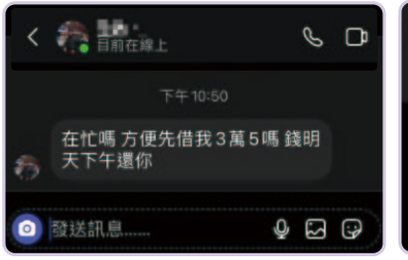
釣魚簡訊及詐騙私訊案例

近年釣魚簡訊也常見於社群媒體與通訊軟體。駭客駭侵帳號，透過他人發送經包裝的發送經包裝的「假活動」、「LINE 輔助認證」或其他不明連結，如「寵物投票大賽」與借錢訊息，利用信任與好奇心進行詐騙。因此，當收到類似訊息時，就算是親友帳號傳的，也務必小心確認與查證，避免被有心人士利用。

防備重點 朋友突然聯絡、訊息夾帶不明網址、LINE 或要求其他服務

⬅傳達虛假的急迫感

⬇不熟的朋友突然聯絡、訊息夾帶不明網址



⬆借錢訊息

⬆不明賣家與購買項目等內容

釣魚電子郵件案例

這是常見的社交工程攻擊手法之一，利用對方的好奇心或製造恐慌的手段，誘導被害人其點擊不明連結或檔案，進而取得其帳密、個資或駭入其裝置。

防備重點

文句不通順、語法奇怪、寄件人 Email 可疑、信件內夾帶不明網址和附件、傳達虛假的急迫感、包含可疑金額

可疑的
電子郵件寄件人➡

userone@elitemed.umgstaging.com

vinicius@ncwbrasil.com.br

⬅ 可疑的金額

金額：52.76 新台幣

⬅ 要求點選連結、奇怪的用語

請單擊此處查找您的運輸跟蹤

⬅ 傳達虛假的急迫感

無法再向您的帳戶添加或接收資金

⬅ 非慣性的奇怪用語

網上銀行

其他釣魚郵件及簡訊的個案

隨著數位化逐漸普及，釣魚郵件及詐騙簡訊的案例也如雨後春筍般不斷出現。除了平時多加防備，也可以透過留意新聞時事，了解新型釣魚信件的不同型態。透過以下提供的數個案例，一同瞭解新型釣魚信件及簡訊慣用的詐騙技巧。

防備重點

手機簡訊認證碼 (OTP) 是常見的認證方式，但駭客可能透過假網站、假訊息騙取 OTP，要求用戶綁定之後，移轉民眾帳戶金錢。
因此在輸入認證碼時，必須謹慎確認來源。

小知識：遇到詐騙怎麼辦？

1. 撥打相關單位 24 小時客服專線，尋求幫助
2. 撥打 165 反詐騙專線
3. 如遇重大錢財損失，立即報警處理
4. 留存證據以方便後續處理

層面三：行動裝置安全

對於現代人而言，同時擁有手機、平板、筆記型電腦等不同行動裝置已是相當稀鬆平常的事。由於其方便攜帶的特性，遭竊、損毀或遺失的機率也很高，而若存有機密資訊、重要個資的行動裝置遭他人盜竊，更將危害自身資安，後果不堪設想。

長期暴露於公共區域的充電 USB，可能遭有心人士竄改設定，例如安裝惡意軟體來竊取個資，因此仍建議隨身攜帶自己的行動電源。

針對行動裝置的詐騙手法：Quishing

Quishing 是指駭客建立一組 QR Code，誘導受害者在不知情的狀況下，掃描或下載其中的惡意內容。由於 QR Code 不易看出隱藏的資訊，若沒有多加留意則很可能會開啟惡意連結。

使用行動裝置的日常習慣

行動裝置易於攜帶、便利性極高的特點，讓身處數位時代的人們往往離不開行動裝置的使用。

這些保護行動裝置安全的好習慣，快來看看您有做到幾項吧！

- ☐ 每週至少關閉並重啟手機一次
- ☐ 盡量不連接免費公共 Wi-Fi
- ☐ 定期清除手機中的 Wi-Fi 連接紀錄
- ☐ 不使用藍牙及 GPS 定位功能時，盡量保持關閉
- ☐ 不輕易開啟陌生信件或簡訊中的網址連結
- ☐ 設定高強度密碼或是採用生物辨識解鎖
- ☐ 選用知名品牌的行動裝置

資安案例

隨著通訊技術發展，資安威脅甚至不需要使用者互動，就能進行駭侵。零點擊攻擊（Zero-Click）利用應用程式的漏洞，隱藏操縱數據的惡意代碼，進而入侵設備；因此需定期更新應用程式或系統，提升設備安全。

使用行動裝置的基本防護措施

除了養成使用行動裝置的良好習慣之外，也應透過行動裝置內建的設定功能，加強設備的基本防護措施，保護自身資訊安全。

關於行動裝置安全的設定及維護，還有一些細節可以再多加留意：

- ☐ 將行動裝置上鎖與定期備份
- ☐ 定期更新軟體與作業系統，避免使用不安全的軟體
- ☐ 避免使用不安全的網路連線方式，例如公共 WIFI 網路
- ☐ 組織內部應建立行動裝置的使用規範
- ☐ 留意裝置停用後的殘存資料，確實刪除資料

行動裝置的其他保護措施

另外，除了上述提到的日常使用習慣及防護措施，也可以選擇其他工具做爲保護隱私及防止個人資料外洩的手段。其中較常見且容易達成的保護措施包含：安裝螢幕防窺片或防窺保護貼、遮蓋裝置的攝影鏡頭等。

◆ 防窺保護貼

◆ 電腦鏡頭蓋

層面四：通訊軟體安全

通訊軟體是日常生活中與外界聯繫的工具，但隨著詐騙手段越來越進步，這也成爲駭客攻擊的管道之一。如果不多加小心，很可能就會成爲下一個「受駭者」！

以下爲幾個常用通訊軟體遭盜用或資料外洩的資安危機實例，幫助大家一起瞭解數種常見的詐騙手段。

社群媒體盜用：LINE 遭盜案例

LINE 是臺灣人最常使用的通訊軟體之一。根據統計，LINE 的使用率在臺灣網路使用者中高達 90.7%，是駭客下手的一大目標。除了直接利用電腦技術駭入使用者帳號，駭客也可能透過詐欺、誘導等手段，讓受害者主動提供簡訊驗證碼等重要驗證資訊。

資料來源：165 全民防騙網

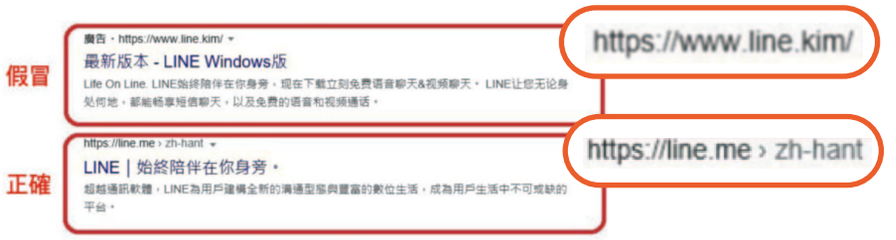
社群媒體盜用：Facebook 遭盜案例

作為臺灣最多網路使用者使用的社群媒體之一（85.3%），Facebook 也是最為人熟知的軟體。然而 Facebook 上的盜用行為，如粉絲專頁遭盜等，除了讓經營者多年的努力付之一炬，有些駭客也會藉此以官方名義向粉絲敲詐，令人防不勝防。

◆ 誘使管理者點擊連結的粉專釣魚訊息

小心！不要亂點假冒的網站！

除了社群媒體，是否也曾在上網搜尋資料時，看過網址非常相似的網站呢？這些網站很可能是「假冒」的網站！曾有駭客刻意設計模仿 LINE 官網，在使用者誤會並點擊進入後，誘導使用者輸入帳號密碼，甚至下載惡意檔案。



帳號資料外洩，帳號安全隨時面臨威脅

即便是上網瀏覽網站，也可能面臨資料外洩的風險。一旦重要資料外洩，駭客便可能趁虛而入，使個資隨時受威脅。

過去幾年，非營利組織、捐助者及其他公民團體資料外洩的案例不時出現在新聞報導上。根據專家分析，駭客為了取得帳號控制權，已經發展出非常成熟的詐欺策略，例如：

1. 假扮成社群網站的支援團隊，向受害者騙取可證明其身分的個資。
2. 若受害者設置兩階段驗證，駭客只要攔截發送驗證碼的簡訊或將驗證碼改發送至駭客裝置上，便能取得帳號的控制權。

時事連結　資料來源：多多益善

上萬公民團體血淚資安事件：NGO 該從哪些小地方著手，維護個案、員工和親友安全？

共享密鑰

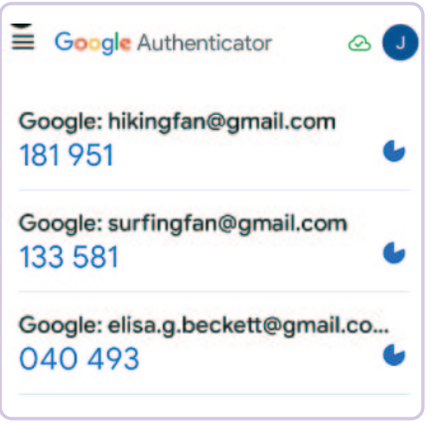
共享密鑰（shared secret）是指在安全通訊傳輸，只有參與通訊的設備才知道的資料。共享密鑰可能是認證密碼、passphrase、大數字，或是一串隨機選擇的陣列。

*passphrase：指詞組密碼，指以自己能記住的隨機字詞或一句喜歡的話組成密碼。

保護帳號安全的好幫手：身分認證機制

身分認證機制，是種用以確認當前使用者爲帳號所有人的一道安全機制。隨著資安議題越來越受矚目，身分認證的方法也越來越多元。登入社群媒體帳號時需要的「共享密鑰」、解鎖手機用到的「生物辨識技術」等都是常見的方法，不同的驗證方法也有不同的安全強度。

身分認證機制採用至少兩種鑑別技術，屬於較強固的安全機制，記得在自己的社群媒體帳號或雲端服務上開啟身分認證機制的「兩步驟驗證功能」，確保帳號不會輕易落入駭客手中喔！



◆ Google推出的Google Authenticator

◆ 登入帳號時可開啟「兩步驟驗證功能」

生物辨識技術

生物辨識技術（Biometric），指透過人體獨特的生理特徵與行爲特徵，來進行數位身分驗證，以及資料存取權控管，其中生理特徵包含指紋、掌紋、虹膜、視網膜及臉部特徵等，而行爲特徵則包含聲紋、簽名辨識等動態特徵。安全風險較低，不僅系統操作便捷，也能有效保障個資安全，目前主要應用於身分驗證和安全控制領域，例如智慧裝置解鎖、行動支付登入、門禁系統等。

層面五：網路服務

現代人相當依賴網路服務，無論是用於儲存資料的 Google 雲端硬碟、線上轉檔網站、ChatGPT 等，都是日常生活和工作中的好幫手。不過，如果輕忽使用這些網路服務的風險，亦有可能導致個人隱私及資料外洩，爲攻擊者所利用。以下將介紹幾個案例，說明網路服務隱藏的資安風險：

線上掃毒工具：只要上傳資料就有外洩的可能

線上掃毒工具有偵測電腦病毒、移除惡意程式等功能，是偵測不明文件及軟體的好幫手。然而，使用線上掃毒工具需將資料上傳至其網頁。若上傳後該資料被有心人士外流至外部伺服器，即有導致個人資料外洩的疑慮。因此，線上掃毒工具雖然方便，但不當使用也可能造成重大資安風險。

時事連結 資料來源：TWCERTCC

使用線上軟體請小心，切勿上傳機敏檔案

線上轉檔服務：實用的面具下，藏著資安風險

線上轉檔服務可將檔案轉換成任意格式，但這同時也意味著使用者主動將資料傳遞到外部伺服器。一旦資料上傳成功，就代表暴露於資料外洩的風險之下。

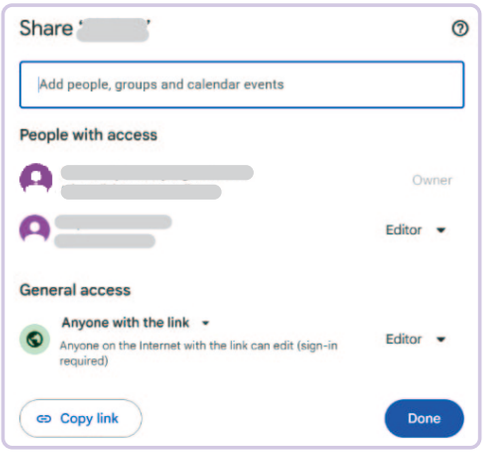
時事連結 資料來源：臺北市政府資訊局

避免使用線上轉檔、加解密服務
以防資安事件發生

善用雲端服務，但也別忘了留意使用安全

雲端服務是指透過網路提供各種服務和資源的線上功能，包括各種伺服器、儲存空間、資料庫和應用程式等，Google 雲端硬碟即爲常見的雲端服務。這些雲端服務雖然方便，且多數服務皆不收費，但如果不多加留意其安全性及正確使用方法，便可能造成資安風險。

- 線上轉檔服務如 PDF 轉換器，是日常生活中常用的服務



- 雲端服務可選擇是否開放權限，爲避免重要資料外洩，記得要隨時留意資料的存取權限

以下是使用雲端服務時可能造成的資安風險，應多加小心並隨時留意，才能保護好資訊安全

1. 錯誤設定重要資料的存取權限，導致沒有權限者也能查看或編輯
2. 員工使用個人帳號執行業務，造成：
   - 公私帳號不分，容易引發資安問題
   - 員工離職後可能會帶走公司的重要資料
3. 雲端服務供應商的安全與可靠度也是一項重要考量
   - 需審慎評估所採用的雲端服務供應商
   - 雲端服務停用後，資料殘存也要及時處理或刪除

服務供應商的疏失：雲端服務安全

儘管使用者萬分小心，仍無法避免雲端服務供應商本身的疏失。過去曾發生大型雲端服務供應商，因硬體損壞或人爲疏忽造成用戶資料大量外洩。類似案例防不勝防，就連全球知名的雲端服務供應商也可能出錯。選擇雲端服務時，需考慮服務供應商的聲譽，以及其提供的服務之安全性與可靠度。

資安案例

美國電信公司因外包商在 AWS 的雲端儲存服務設定錯誤，導致 600 萬用戶隱私有遭洩密之風險，包含用戶姓名、地址與驗證密碼，一旦遭洩密，將影響用戶甚鉅。

未來的資安風險：生成式 AI 服務

生成式 AI 自從問世後，便成爲民衆常用的網路服務之一。如 ChatGPT、簡報製作 AI 服務 Gamma，都是近來熱門的 AI 服務。儘管生成式 AI 用途廣泛，其安全性仍有待觀察；如果未來遭到攻擊者或駭客濫用，勢必會成爲新的資安攻擊工具，衍生出不同的攻擊模式與手段。此外，若在 ChatGPT 等生成式 AI 服務上傳機密資料，也可能造成資料外洩。

◆ OpenAI 的 ChatGPT 服務

資安案例

韓國知名手機製造商發現，旗下工程師將內部原始碼上傳至 ChatGPT。爲避免公司敏感資訊上傳至外部服務，規定員工不得於公司內網使用生成式 AI 系統。

層面六：實體安全

資訊安全不僅關乎軟體、亦包含硬體的實體安全。實體安全是指保護硬體設施、設備及資產設備等，以防受到破壞、未授權的存取、偷竊或其他潛在威脅。硬體常見的安全威脅包括以下四種：

1. **天然環境災害**
   例如水災、颱風、地震、土石流、山崩及極端氣候等
2. **能源供應系統中斷**
   這些能源包括電力、水資源、通訊等
3. **人爲的破壞**
   例如火災、非法入侵、破壞、偷竊、爆裂物、員工疏失等
4. **政治事件**
   例如戰爭及衝突、抗議活動、恐怖組織的襲擊等

◆ 高壓電塔、水壩等都是重要的電力來源，確保供應穩定也是實體安全的防護方法

實體安全的防護措施：我們可以怎麼做？

對硬體設備來說，防護措施是確保資訊安全不可少的環節，那究竟可以採取什麼樣的防護措施進行有效保護呢？一起來看看有哪些防護方法吧！

實體安全的防護事項，來看看有做到哪些吧!

1. **建立實體屏障：**例如圍欄、門、鎖、防盜窗等
2. **對人員進出進行管制：**例如對來往人員進行身分認證、訪客進出登記、記錄人員進出
3. **建立監控系統：**例如建立攝影監視系統、環境監控(室內的溫溼度)
4. **配備警報系統：**例如入侵警報、火災警報等
5. **足夠的安全照明，嚇阻潛在的入侵者**
6. **配備足夠的警衛人員**
7. **加強對設備的保護：**加強對關鍵資訊設備的保護，如：伺服器機櫃，以及建立設備攜入 / 攜出的管制程序
8. **建立火災防範措施，確認消防設備沒有損壞**
9. **確保電力來源供應穩定：**確保不斷電系統、發電機運作穩定，沒有其他抗電力干擾

設備淘汰之後：務必刪除資料或是停用帳號

硬體設備和資訊設備都有使用壽命，在丟棄或淘汰這些設備前，應先將重要資料徹底刪除或進行實體破壞，以防重要資料意外洩露到他人手上。

另外，如果設備要移作他用或是捐贈於他人，則應在轉手之前確認儲存在其中的資料不可再讀取，防止有心人竊取資料。

資安案例

美國知名財富管理機構在關閉部門時，未能妥善處理擁有客戶個資的重要系統，聘請了一家不具資料銷毀專業的公司，報廢數千台硬碟與伺服器，導致客戶個資遭轉賣至拍賣網站。

實體安全受危害：紙本資料管理不當

正如前述所言，紙本也是其中一種實體儲存方式，因此也需要注意實體安全的防護措施。然而，實體的紙本資料在資料儲存上具一定難度，也容易因管理不當，經常成爲資料外洩的主因之一。

層面七：委外安全

將業務外包給第三方供應商難免涉及機密資料，業務外包會面對的委外安全，成爲不可避免的重要議題。下面將提供業務委外需注意的事項，並介紹幾個案例，讓大家快速了解業務外包可能存在的資安風險。

如果您有業務委外的需求，以下是可以參考的注意事項

1. 謹慎選擇具信譽且可信賴的第三方供應商
2. 雙方合作開始前，簽訂全面的資安與保密協議
3. 隨時留意業務委外過程中的資料保護
4. 確認委外過程中的合規性和法律責任
5. 委外結束後，應謹慎處理後續資料，採取實體銷毀或確保第三方供應商無法再次讀取重要資料

案例探討

資料來源：中央社

知名電視台片庫資料
遭廠商誤刪 8 萬筆

事件概要

2022 年 3 月，某電視台因內部缺乏專業資安專業人才，將新的儲存系統建置工作外包給第三方廠商。

事件經過

儲存系統建置過程中，廠商在未告知甲方的情況下，自行決定於系統安裝遠端控制軟體。

事件結果

廠商在未經甲方同意的情況下執行了可能刪除資料的指令，導致 42 萬多筆新聞資料遭到廠商誤刪。加上過程中缺乏完整的備份程序，許多被刪除的資料無法完整復原。

委外安全的保護辦法：重要區域應嚴格進行出入控管

委外安全面對的最主要威脅，在於無法確定委外的第三方廠商，是否會濫用外包的資料。爲了減低外包業務帶來的資安風險，應針對重要區域進行人員進出管制。具體做法爲讓廠商進入重要區域前，先了解並同意資安政策，防止廠商帶走重要資料、攜帶不符資格的設備、違反資安政策等行爲。


線上文件填寫系統

入廠時間：2024/05/17　IP Address：
公司名稱：　姓名：　聯絡電話：
E-Mail Address：

I. [redacted] 安全政策、訪客須知及入廠須知

資訊安全政策及訪客須知 (請詳閱內容)

1. 禁止攜入下列物品：沒有安裝防毒軟體的電腦設備、具照相/攝錄影功能的設備、非工作相關之具儲存功能之電子設備與媒介，以及具資料傳輸功能的網路設備。
2. 違規攜入處罰：台幣二千元；[redacted]廠區內最高處罰台幣二十萬元。
3. 攜出之電腦設備無彌封、彌封損毀或與登記數量不符者，離廠時須執行格式化作業，並罰款台幣二千元。
4. 若經查攜訪客攜出未經授權之[redacted]資料，或攜入之儲存媒體、電腦與網路相關設備，被發現病毒或其他原因造成難電的損失，本公司將依損害程度追行求償。

◆ 某一企業要求訪客在入廠之前填寫個人資料，並同意相關的資安政策及須知事項

資訊安全政策與訪客須知（節錄）

1. 禁止攜入下列物品：沒有安裝防毒軟體的電腦設備、具照相 / 攝錄影功能的設備、非工作相關之具儲存功能之電子設備與媒介，以及具資料傳輸功能的網路設備。
2. ....
3. 攜出之電腦設備無彌封、彌封損毀或與登記數量不符者，離場時需執行格式化處理 ...

層面八：人力資源安全

除了硬體與軟體的安全之外，也應留心設備操作人員，避免內部成爲破口，外洩重要資料及機密文件。

以下是企業及非營利組織在招募人力的流程中需留意的細節，以盡可能減少人力資源帶來的風險

聘僱前

- 評估員工的身分、學經歷、專業資格乃至道德操守，避免品行不佳的員工影響企業營運及形象
- 要求員工提供良民證等可證明自身道德品行的官方文件

應聘

- 告知企業的工作規範、義務責任與資安政策
- 定時提供員工教育訓練，培養員工的資安意識及對資安的重視

離職

- 離職後員工應落實相關要求，將帳戶個資、實體鑰匙、帳戶權限等歸還於企業或組織
- 離職後員工不應私自保留任職期間在企業和組織取得的資料

企業及非營利組織除了應定時加強員工的教育訓練、培養員工對資安的正確觀念及安意識，也要培養徹底關閉離職人員權限的習慣，以杜絕其再登入下載資料的可能。

結語

資安的基本防護作為人人都可以做得到!

相信在了解資安及相關的安全概念後，大家對日常生活、工作職場上的資安議題都有更清晰的認識。

資安看起來艱澀難懂，可能會讓一般人知難而退，然而我們在日常上其實就能採取許多資安防護行爲，也不如大家想像的困難。

以下，將帶大家回顧我們可以落實的基本資安防護行動，只要時時謹記這些原則及做法，就能大大減低可能面臨的資安風險。

只要是機密，就不可隨意亂傳!

常見機密資料包含使用者帳密、內部加密資料等，只要牽涉機敏資訊或相關機密文件，就必須多加留意。尤其是在使用網路及雲端服務時，應避免將機密文件上傳到未經認證的網站，或透過非加密方式傳遞給他人或外部網站，以免造成機敏資訊外洩。

重要資料加密、加密、再加密!

生活中或工作上互相傳遞資料十分常見，甚至是必要的網路行爲。不過在儲存或傳輸重要資料之前，切記要先將這些資料進行加密處理。

強化資料存取與控制的安全機制

對於機密資料或重要文件，應實施更全面且嚴格的權限管理機制。例如，當有人需要取得資料或系統的使用權限時，先進行身分驗證；進出重要資料的儲存場所時，需做好實體的進出人員管制等。而針對經常使用的帳號，除密碼需符合基本複雜度要求外，也別忘了開啟雙因子驗證（2FA）、多因子驗證（MFA）等身分認證機制。

3–2–1 法則：對抗資料遺失

指「重要資料應至少備份 3 份、備份資料應分別儲存於 2 種不同的存放媒體、其中一份需置於異地存放」。徹底實踐 3-2-1 的備份法則，才能避免受到網路攻擊時，備份資料遭受攻擊或遺失的風險。

企業及非營利組織，又能怎麼做？

1 制定資安管理的具體規範及機制

除了以上的基本防範措施外，企業及非營利組織也需制定更嚴格的資安管理規範及方法，並且嚴格監督、徹底落實。如針對員工資訊裝置建立使用及管理規範、制定委外安全管理 SOP 等，以封堵管理上的安全漏洞，盡可能降低受到攻擊的風險；同時對於資安攻擊事件也應做好全面準備，制訂完善的應對計畫。

2 落實基本的資安防護措施

企業及非營利組織應重視並落實基本的資安防護措施，例如：定期更新裝置的作業系統與應用程式，避免漏洞遭駭客利用。此外，公用電腦、員工個人筆電等資訊裝置都必須安裝防毒軟體，防止惡意軟體從端點感染整個內部網路。

3 定期進行教育訓練

從員工入職前、任職中到離職後的任一環節，資安意識與教育訓練都對維護資訊安全有重要的作用。企業與非營利組織除了提供完整、專業的教育訓練外，也應定時進行無預警的突擊演練，確保所有員工將資安的防護知識落實於日常行爲中。

最後的最後
防範資安攻擊的終極方法
就是注意、注意、再注意!

參考資料

1. 超過六成被駭台灣中小企業遺失客戶數據，修復是大挑戰
https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=9522

2. 2024企業最需警戒的資安風險
https://www.ithome.com.tw/article/162252

3. Fortinet：逾六成企業曾因採行遠距工作模式而發生資料外洩
https://www.fortinet.com/tw/corporate/about-us/newsroom/press-releases/2023/foritnet-release-wfa-suervey-and-announces-sase-enhancement

4. Arbor Networks發現了鎖定亞洲幾國政府及NGO組織的多段式攻擊活動
https://www.ithome.com.tw/pr/103359

5. 中小企業成駭客新目標！盤點企業必備的資安防護3大基本觀
https://buzzorange.com/techorange/2023/04/21/cyber-threats-to-small-businesses/

6. 2.5萬筆學習歷程檔案遺失 教部：將補助教師輔導學生重製
https://www.cna.com.tw/news/firstnews/202109260043.aspx

7. 「我的愛心被駭客利用了！個資外洩風暴下，公益團體的重建信任之路
https://www.twreporter.org/a/personal-data-leaked-npo-donators

8. 國家資通安全研究院：勒索軟體防護
https://www.nics.nat.gov.tw/cybersecurity_resources/promotional_resources/Protection_Guide/Ransomware_Protection/

9. 不明簡訊「衛福部提供確診者補助金」爲詐騙訊息
https://www.mohw.gov.tw/cp-4343-71097-1.html

10. 上萬公民團體血淚資安事件：NGO 該從哪些小地方著手，維護個案、員工和親友安全？
https://rightplus.org/2022/07/21/security/

11. [警訊]使用線上軟體請小心，切勿上傳機敏檔案
https://www.twcert.org.tw/newepaper/cp-65-609-b1e03-3.html

12. 請同仁避免使用線上轉檔、加解密服務，以防資安事件發生
https://doit.gov.taipei/News_Content.aspx?n=9B8993131395DA3F&sms=93D47212F58C7A57&s=46FD091DEE0322E4

13. 知名電視台片庫資料遭廠商誤刪 8萬筆遺失
https://www.cna.com.tw/news/amov/202203150048.aspx

《資安星際指南：資安基礎概論》

出版單位	國家資通安全研究院
召 集 人	林盈達
主　　編	許建榮
副 主 編	鄭瑋
執行編輯	胡馨元
作　　者	邱元貞、張恩鳳、陳思帆、謝采軒
審　　訂	鄭郁翰、郭怡伶
設　　計	施逸青
特別感謝	社團法人台灣數位外交協會
出版日期	2025 年 8 月　初版一刷
ISBN	978-986-5436-67-4

本手冊由 Google.org 提供資金挹注「NICS 台灣資安計畫」出版
國科會計畫補助編號 MOST113-2627-M-002 -001 - 補助

本手冊中所提供的外部資訊及相關連結，其責任與權利歸屬於該媒體單位或作者所有

國家資通安全研究院
National Institute of Cyber Security

with support from Google.org

ISBN: 978-986-5436-67-4