臺北市政府教育局

114年度委外辦理資訊安全暨個人資料隱私保護驗證案

資安通識及個資保護安全認知宣導課程

KPMG Shawn Yin

114.08

尹大湘 Shawn Yin

經歷

- ✓現任KPMG台灣所 顧問服務部 顧問師
  資訊安全管理系統專案諮詢服務
- ✓實踐大學 企業管理研究所碩士

專業資格

- ✓CISA國際認證電腦稽核師
- ✓ISO 27001：2022 主導稽核員轉版證書
- ✓ISO 27001 資訊安全管理系統主導稽核員
- ✓ISO 27701 隱私資訊管理系統主導稽核員
- ✓ISO 42001 人工智慧管理系統主導稽核員
- ✓資通系統防護基準合規自評師認證

服務經歷

- ✓臺北市政府教育局　委外辦理資訊安全暨個人資料隱私保護驗證
- ✓臺北市政府人事處　資訊安全管理系統維護及驗證委外服務案
- ✓數位發展部　資訊安全管理系統及個人資料隱私管理系統維運作業服務案
- ✓交通部公路局　資訊安全、資訊服務與個資保護管理制度輔導及驗證委外案
- ✓交通部高速公路局　資訊安全暨個人資料保護管理制度委外服務案
- ✓統一速達股份有限公司　資訊安全管理系統與個資保護管理顧問案

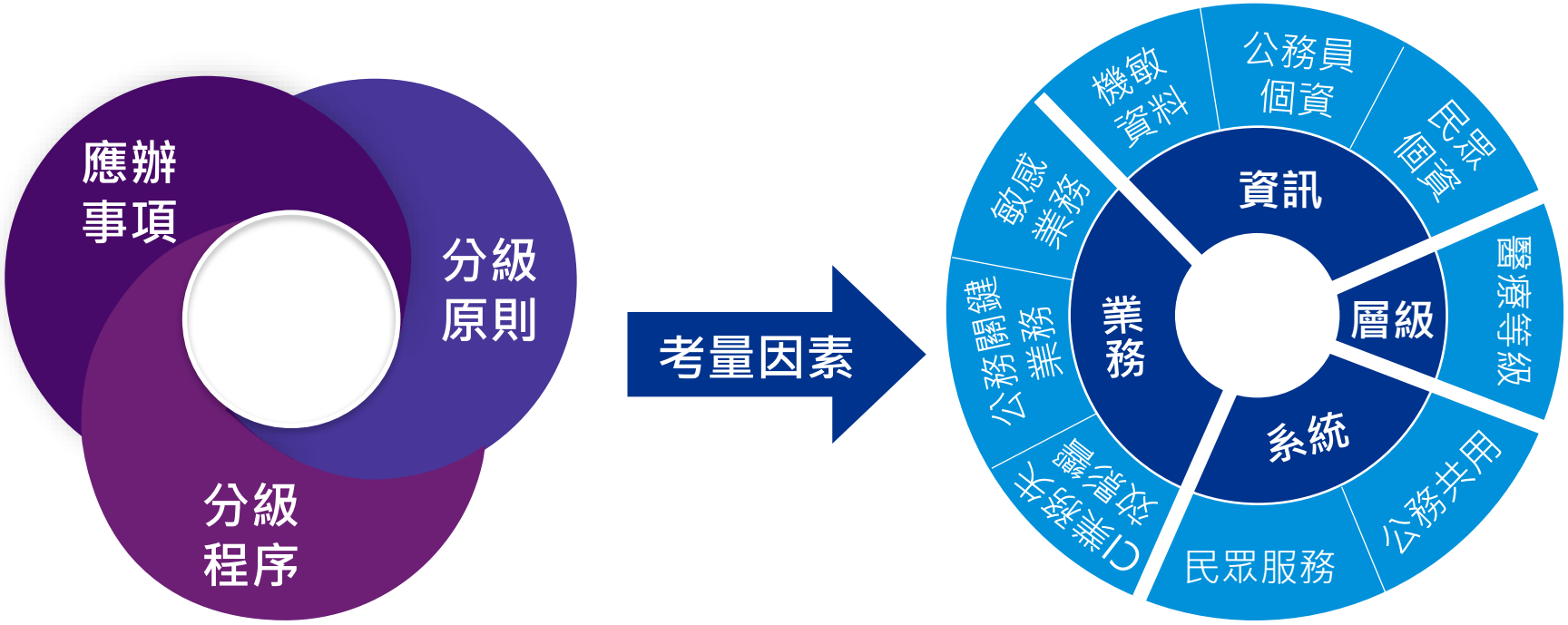
簡報大綱

1	本局資安規定及具資安疑慮產品宣導
2	近期資安暨個資案例說明(Case Study)
3	社交工程認知與宣導
4	新興議題分享
5	問題與討論 Q & A

本局資安規定及具資安疑慮產品宣導

資通安全責任等級分級辦法簡介

- 機關應考量其**業務、資訊、系統、機關層級**等因素訂定機關資安責任等級
- 後續依該責任等級辦理相對應之應辦事項



資通安全責任等級分級原則

A級 全國性

B級 區域或地區性

C級 有自行或委外開發資通系統，並設置伺服器者

D級 未自行或委外開發資通系統，未設置伺服器

E級 全部資訊業務由其他機關兼辦或代辦

各責任等級應辦事項(管理面)

責任等級		資通系統分級及防護基準	資訊安全管理系統之導入及通過公正第三方之驗證	資通安全專責人員	內部資通安全稽核	業務持續運作演練	資安治理成熟度評估
B	公務機關	1年內完成	•2年內導入CNS 27001資訊安全管理系統國家標準 •3年內完成公正第三方驗證	2人	1次/年	1次/2年	1次/年
	特定非公務機關	1年內完成	•2年內導入CNS 27001資訊安全管理系統國家標準 •3年內完成公正第三方驗證	2人	1次/年	1次/2年	--
C	公務機關	•1年內完成資通 系統分級 •2年內完成防護基準	•2年內導入CNS 27001資訊安全管理系統國家標準	1人	1次/2年	1次/2年	--
	特定非公務機關	•1年內完成資通 系統分級 •2年內完成防護 基準	•2年內導入CNS 27001資訊安全管理系統國家標準	1人	1次/2年	1次/2年	--
D級之各機關		--	--	--	--	--	--

各責任等級應辦事項(管理面)

責任等級		安全性檢測		資通安全健診	資通安全監控管理機制	政府組態基準	資通安全防護					
		網站安全弱點檢測	系統滲透測試				防毒軟體	防火牆	郵件過濾	入侵偵測及防禦機制	應用程式防火牆	進階持續性威脅攻擊防禦措施
B	公務機關	1次/年	1次/2年	1次/2年	√	√	√	√	√	√	√	--
	特定非公務機關	1次/年	1次/2年	1次/2年	√	--	√	√	√	√	√	--
C	公務機關	1次/2年	1次/2年	1次/2年	--	--	√	√	√	--	--	--
	特定非公務機關	1次/2年	1次/2年	1次/2年	--	--	√	√	√	--	--	--
D級之各機關		--	--	--	--	--	√	√	--	--	--	--

3家銀行違反個資法或內控規定 金管會裁罰

- 中信銀行的3名行員因非基於業務需求私下查詢客戶個資，因違反個資法被金管會罰款新台幣12.5萬元。
- 金管會證期局在檢查大展證券時發現5項缺失，包括：未經授權代理客戶下單、未將參與自營部門每日晨會的董事納入利益衝突檢核對象、未訂定執行高齡客戶外的他人以電話代指示交易的管控措施、外部人員遠端連線管理規範不完備、未訂定個資檔案安全維護計畫及業務終止後個資處理方法。最終證期局決議對大展證券罰款新台幣54萬元。
- 證交所與券商公會查核永豐金證券敦北分公司時，發現業務員違規接受客戶全權委託且未依客戶指示下單，證期局決議對永豐金證券罰款新台幣48萬元。

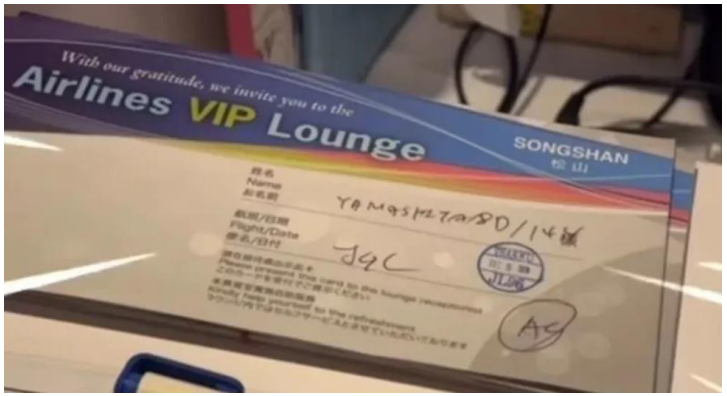
注意事項

- 確保所有查詢和處理個人資料的行為都基於合法授權，並且有明確的業務需求。未經授權的查詢或處理個人資料是違法的
- 嚴格管理和監控業務員接受客戶全權委託的行為，確保所有交易都依據客戶的明確指示進行

資料來源：yahoo新聞 2024.02.06

山下智久個資遭外洩！松機「貴賓室員工」PO限動 營運商道歉了

- 日本男星山下智久在松山機場貴賓室休息時，遭一名貴賓室員工拍下其貴賓室憑證、搭乘航班及座位等個資，並將照片PO上社交媒體，引發網友關注與討論。
- 該貴賓室營運商高雄空廚對此事作出道歉，表示已要求員工刪除照片並進行調查，承諾將依公司規定對該員工進行處分，並加強員工教育訓練。
- 事件引發社會輿論關注，認為此行為不當，且此類行為可能對當事人造成困擾。山下智久及其經紀公司尚未公開反應



注意事項

- 這起事件突顯了企業在處理敏感資料和員工管理上的不足，尤其是在個人資料保護方面。對員工的教育訓練應強化，避免未經授權的資料洩漏。
- 員工將客戶的個人資訊公開至社交平台，這樣的行為可能違反隱私法律規範，需依照相關法律負責。

資料來源：yahoo新聞 2024.02.06

個人資料保護法(部分)

第 1 條
為規範個人資料之**蒐集、處理及利用**，以避免人格權受侵害，並促進個人資料之合理利用，特制定本法。

第 4 條
受**公務機關或非公務機關委託**蒐集、處理或利用個人資料者，**於本法適用範圍內**，視同委託機關。

第 5 條
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**。

個資的生命週期

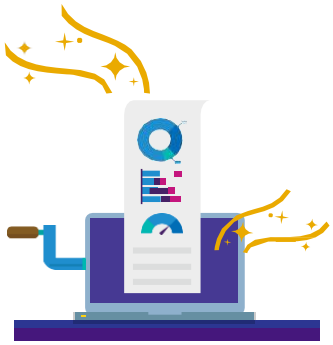
指以任何方式取得個人資料。

指將個人資料委由他人進行處理。

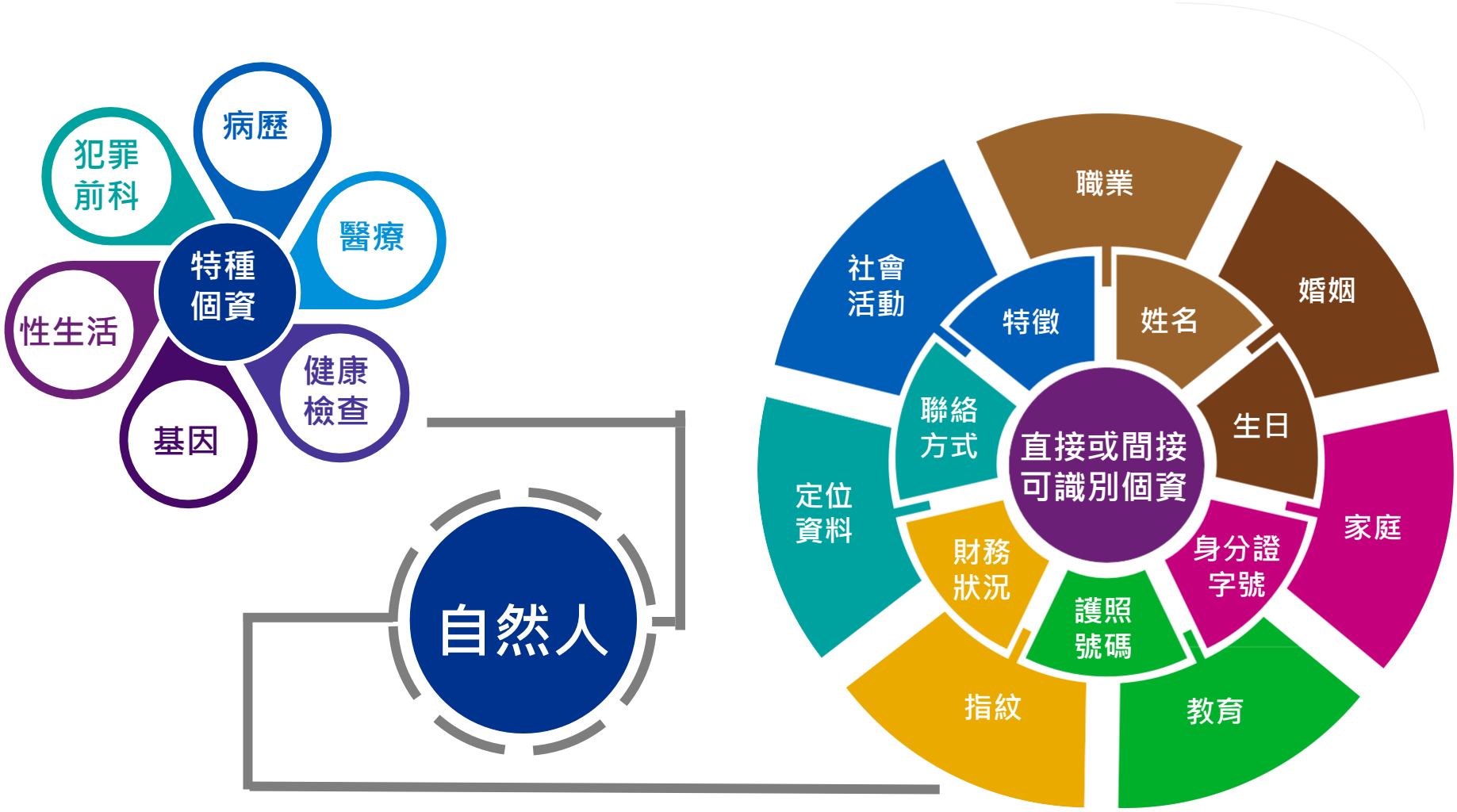
指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。

指將蒐集之個人資料為處理以外之使用。

指將蒐集之個資進行刪除。



個人資料類別



具資安疑慮產品之宣導事項(1/4)

行政院秘書長109年12月18日院臺護長字第1090201804A號函重點如下：

使用資通訊產品(含軟體、硬體及服務)相關原則如下：

- 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**。
- 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**。
- 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**。
- 各機關「從嚴認定」，所有大陸廠牌者，無論原產地於**我國**、**大陸地區**或**第三地區**等，均需納入填報範圍。
- 盤點包含軟體、硬體、服務，另具有**連網能力**、**資料處理**或**控制功能者**，如無人機、網路攝影機、印表機。

具資安疑慮產品之宣導事項(2/4)

行政院國家資通安全會報第36次委員會議(擴大會議)決議重點如下：

- 定期並**擴大**辦理大陸盤點作業，包含全機關、委外廠商、複委託廠商及其使用之資通訊設備。
- 各機關於辦理採購時，應確實於招標文件規定**不允許大陸地區廠商**參與，並**不得採購大陸廠牌**資通訊產品。
- 公務設備**不得下載安裝**大陸地區軟體(含APP)，公務活動**不得使用**大陸地區所提供之平台或服務。
- 請同仁**避免購買或使用**大陸廠牌資通訊產品，並落實要求大陸廠牌資通訊產品一律禁止處理公務或介接公務環境。
- 如有採購大陸廠牌資通訊設備，應於109年底前完成汰換作業，汰換前**不得與公務環境介接**。
- 大陸廠牌認定：為**大陸品牌**，無論其原來產地為何。
- 勿使用**大陸廠牌USB隨身碟**連接公務資通訊設備。

具資安疑慮產品之宣導事項(3/4)

行政院中華民國114年3月31日院授數資安字第1141000253號函重點如下：

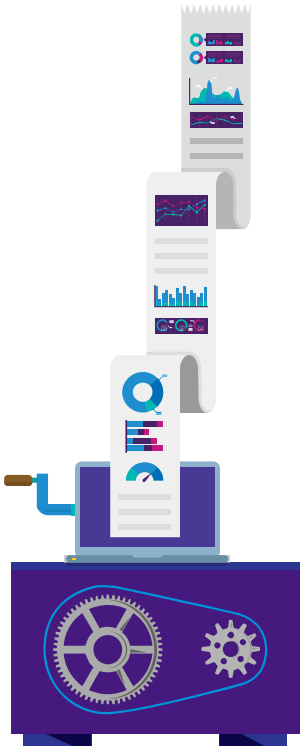
- 為避免公務及機敏資料遭不當竊取，導致機關機敏公務資訊外洩或造成國家資通安全危害風險，行政院前已發布「**各機關對危害國家資通安全產品限制使用原則**」，明確要求中央與地方機關（構）、公立學校、公營事業、行政法人以及自行或委外營運提供公眾活動或使用之場地，限制使用危害國家資通安全產品
- 並以行政院秘書長109年12月18日院臺護長字第1090201804A號函，重申公務用之資通訊產品不得使用大陸廠牌，且不得安裝非公務用軟體。
- 為因應新型態數位服務延伸之新興資安風險，再次重申各公務機關應遵循前述規定，並請配合辦理以下事項：
  1. 公務用之資通訊產品**不得使用大陸廠牌**，且**不得安裝非公務用軟體**。
  2. 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**。

具資安疑慮產品之宣導事項(4/4)

行政院中華民國114年3月31日院授數資安字第1141000253號函重點如下：

3. 前開產品未汰換前，應有適當配套措施或相應作為，例如：以不含個資及資料的電腦單機將其下載並以斷網或非公務網路之獨立網路使用、強化資安管理措施(如：設定高強度密碼、禁止遠端維護等)

- 公務機關原則全面**禁用Deepseek AI等大陸廠牌資通訊產品**，倘因業務需求且無其他替代方案，必須採購或使用前開產品時，應具體敘明理由，經機關資安長及其上級機關資安長逐級核可，函報《資通安全管理法》主管機關數位發展部核定後，以專案方式購置列冊管理。另教學及研究場域之使用原則，則依教育部與國家科學及技術委員會另定規範辦理。



KPMG

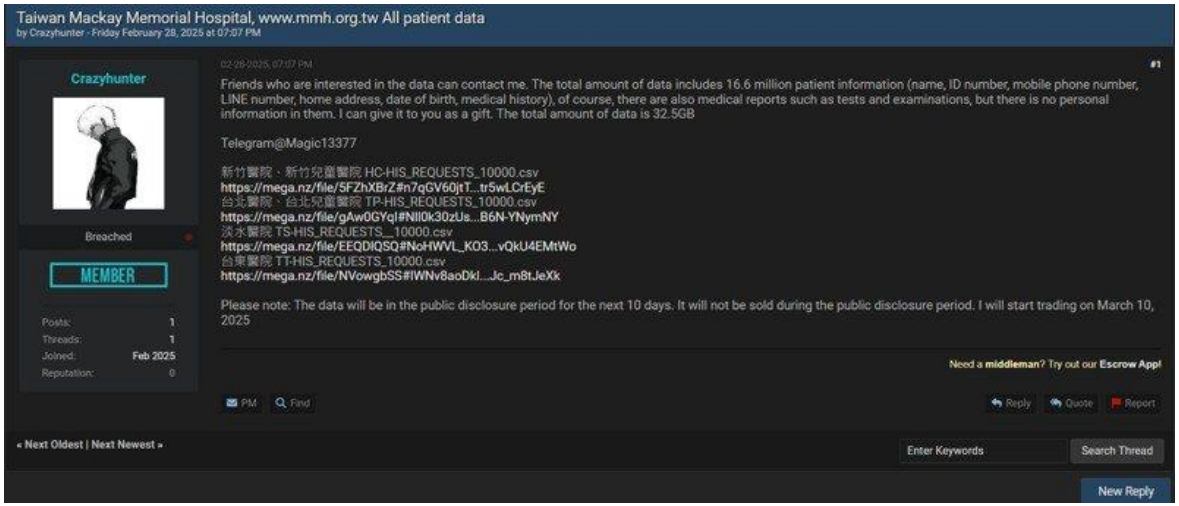
近期資安暨個資案例說明 (Case Study)

KPMG

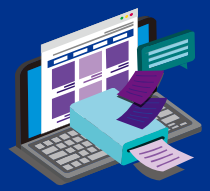
近期資安暨個資案例 1
機敏個資外洩

馬偕1660萬名病人個資恐外洩 駭客集團開價309萬元賣出

駭客這次在**暗網上又放上1660萬筆的馬偕醫院病歷資料**，這一次被洩露的資訊，包含**姓名、身分證字號、手機號碼、住家地址、病歷**。駭客透過馬偕醫院的內部作業電腦入侵，藉由勒索軟體**來取得機敏資料的權限和通道，導致馬偕醫院病歷資料於暗網被公開販售。**



資料來源：聯合報 2025/03/05

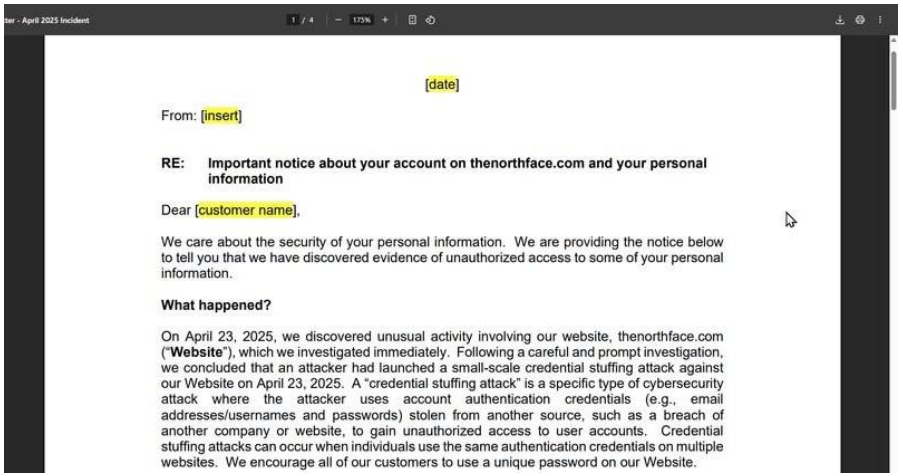


戶外用品與運動服飾業者The North Face遭遇帳號填充攻擊，部分客戶個資外洩

The North Face 官方網站遭遇「帳號填充攻擊（Credential Stuffing）」，導致部分客戶個資外洩，包括**姓名、購買紀錄、地址、Email、生日與電話**。該公司於5月29日向佛蒙特州總檢察長通報此事，並通知受影響用戶。雖然付款資訊未受影響，但這已是該品牌自2020年以來多次遭遇類似攻擊，資安專家指出，未強制實施多因素驗證（MFA）可能是主因之一。

KPMG觀點

- 實施MFA機制：降低帳號被盜風險
- 偵測異常行為：如短時間內大量登入失敗、異常 IP 存取。
- 限制暴力破解：加入 CAPTCHA、IP 封鎖等機制。
- 強化通報機制：一旦發現資安事件，應即時通報並通知用戶。



[date]

From: [insert]

RE: Important notice about your account on thenorthface.com and your personal information

Dear [customer name],

We care about the security of your personal information. We are providing the notice below to tell you that we have discovered evidence of unauthorized access to some of your personal information.

What happened?

On April 23, 2025, we discovered unusual activity involving our website, thenorthface.com ("**Website**"), which we investigated immediately. Following a careful and prompt investigation, we concluded that an attacker had launched a small-scale credential stuffing attack against our Website on April 23, 2025. A "credential stuffing attack" is a specific type of cybersecurity attack where the attacker uses account authentication credentials (e.g., email addresses/usernames and passwords) stolen from another source, such as a breach of another company or website, to gain unauthorized access to user accounts. Credential stuffing attacks can occur when individuals use the same authentication credentials on multiple websites. We encourage all of our customers to use a unique password on our Website.

資料來源： iThome 2025-06-04

中製APP資安風險高，資安院提醒民眾慎選使用，避免個資外洩

我國國安局、法務部調查局及警政署刑事局依據數發部發布的「行動應用APP基本資安檢測基準v4.0」指標，對小紅書、微博、抖音、微信及百度雲盤共5種中國APP進行檢測，發現皆出現多項高風險行為，類型包含**「蒐集敏感性資訊」、「讀取儲存空間」、「逾越APP使用功能之權限」、「擷取系統資訊」、「掌握生物特徵」以及「數據回傳與分享」**等6大面向，顯示中製APP在資安防護上仍有重大疑慮。

資安院建議

- 安裝APP前，詳閱權限要求與隱私條款。
- 定期檢查手機APP權限設定，關閉不必要的權限。
- 優先選用來源可信之APP，避免安裝來路不明程式。
- 使用資安防護工具，監控資料傳輸與異常行為。
- APP要求提供機敏資訊前，應評估其合理性與必要性。

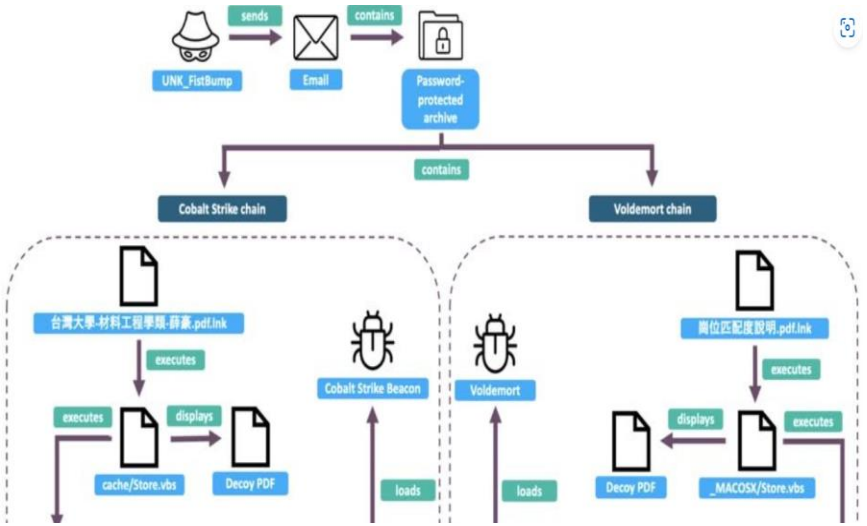
資料來源：國家資通安全研究院 2025-07-04

中國駭客鎖定臺灣半導體生態系從事大規模網釣，假冒研究生求職與投資分析合作

半導體是臺灣的經濟命脈，中國在面對美國技術封鎖與制裁下，急於發展自主半導體技術。近期資安公司 Proofpoint 發現，中國國家支持的駭客組織正透過網路釣魚手法，試圖竊取臺灣半導體產業的機密資訊。

攻擊手法

- **誘餌**：假冒臺灣大學畢業生求職信
- **手法**：使用遭入侵的大專院校信箱寄送履歷，內含惡意連結
- **後果**：下載檔案後植入 Cobalt Strike / Voldemort 後門程式
- **攻擊者**：疑中國駭客組織 TA415 有關

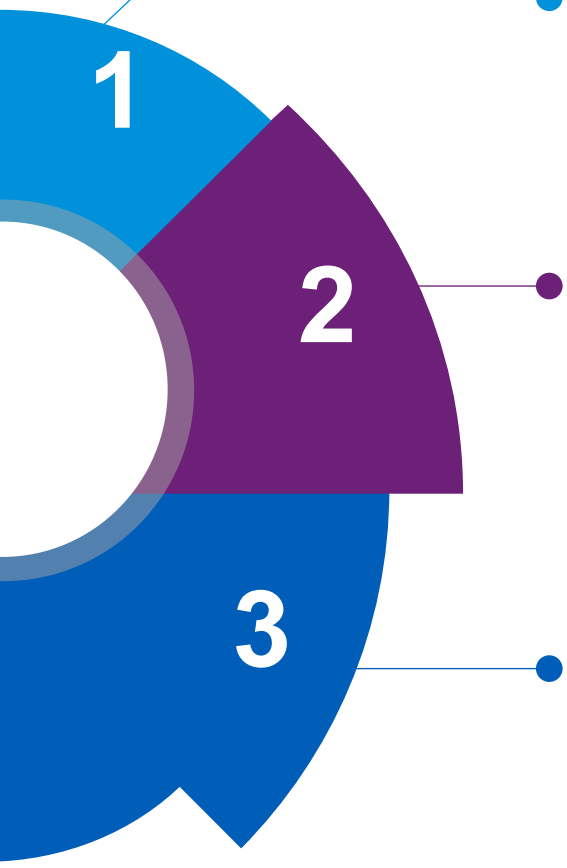


資料來源：iThome 2025-07-18

資料外洩會發生什麼事?

- 破解其他使用相同帳密的帳號。
- 登入你的網路銀行帳號來取走資金。
- 以你的名義辦理銀行帳號/信用貸款，會影響你的信用評等。
- 以你的名義訂手機或將你的SIM卡轉到新裝置。
- 以你的名義購買昂貴物品用於犯罪轉賣，通常是透過劫持你在電子零售商的網路帳號進行。
- 提交虛假的退稅單，以你的名義收取退稅。
- 利用你的保險詳細資料進行醫療服務。
- 入侵工作帳號來攻擊你的雇主。

造成資料外洩常見原因(1/2)



◆ 網路釣魚攻擊

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。

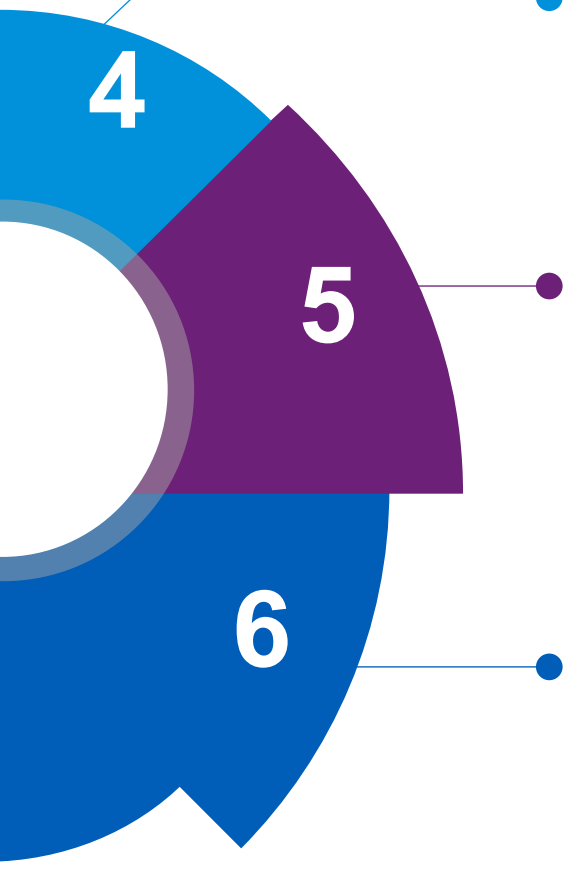
◆ 盜用帳號

當Apple ID或Google帳號、Amazon或樂天等購物網站、Facebook或LINE等社群網站的帳號被盜用時，可能導致**資料外洩**，或是盜用帳號者**假冒您的身分竊取資訊**之風險，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。

◆ 終端裝置遭竊或遺失

有歹徒專門竊取裝置或在公共場所找尋別人**遺失/亂放的裝置**，在電腦或智慧型手機中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，可能會發生未授權操作而導致這些個資發生外洩。

造成資料外洩常見原因(2/2)



◆ 惡意軟體或惡意應用程式的未授權操作

病毒等惡意軟體或惡意應用程式的**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。

◆ 在社群網站上過度公開資訊

當使用Facebook、Instagram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**，但除了朋友以外也存在專門收集資訊的不特定人事，會將資料用於犯罪用途，或賣給惡質的個資名單業者。

◆ 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。此外，也有創造與公共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。

如何防範資料外洩？

KPMG建議

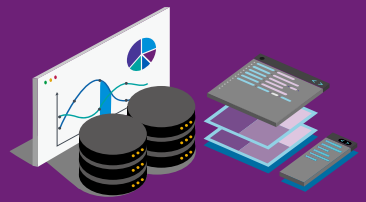
- ✓ 不應直接以容易被猜出的自身個資作為密碼，以免帳號遭盜用。
- ✓ 對重要帳號開啟**雙重認證**登入，以確保登入者為本人，多一層保障
- ✓ 請密切注意自己的**銀行帳號信用卡**是否有異常的支出活動。
- ✓ 針對包含任何連結的訊息必須謹慎對待，**切勿**點開不請自來郵件內的連結或附件檔。
- ✓ 網路購物前先確認網站是否有開啓**SSL加密**(https)。購物完成後不要留存信用卡資料在它方。
- ✓ 為所有的電腦和行動裝置安裝知名廠商的**防毒軟體**。
- ✓ 確保所有的作業系統和應用程式都保持在**最新版本**（即經常更新修補程式）。
- ✓ 切勿在社群媒體上過度分享，也盡量避免**使用公共Wi-Fi**上網，如使用公共Wi-Fi上網時，不要進行網路購物、網上銀行、收發電子郵件等涉及帳號登錄行為之操作。

請記住，如果在網路上看到東西好的太不真實，
那通常就是假的！！

帳號被盜急救指南 (1/3)

更改密碼

- 通常是因為駭客取得了我們的帳號密碼，**透過更改密碼**，我們可以讓駭客手上的密碼失效，無法再登入我們的帳號。



開啟多因子認證

- 多因子認證登入時不僅需要密碼，還要取得我們的**手機驗證碼或是實體金鑰**，這會讓攻擊的困難度增加很多，提高帳號的安全性。

登出所有的裝置

- 把已經登入在帳號內的人都剔除，**強迫他們必須重新透過帳號密碼驗證身份**，避免駭客更改密碼以後繼續潛伏在我們的帳號。

帳號被盜急救指南 (2/3)

檢查帳號上異常活動

- 駭客有無透過入侵社群帳號，傳釣魚訊息給我們的朋友。**檢查帳號設定，資訊有沒有被修改、備用Email或電話有沒有被改成駭客的資料。**

檢查自己其他的帳號

- 駭客會利用被入侵的帳號上來搜集資訊，並**試著攻擊你的其他帳號**。除了檢查被入侵的帳號外，也要檢查其他常用重要的帳號。

檢查電腦有沒有中毒

- 透過**防毒軟體來掃瞄電腦**，檢查是否有惡意程式。若真發現了電腦有中毒的話，記得要再**更改一次被盜的帳號的密碼**。

帳號被盜急救指南 (3/3)

警告親朋好友

- 透過入侵一個人的社群帳號後，用**他的名義傳送大量的訊息給其他好友**。因為是認識的人傳來的訊息，受騙上當點開惡意連結或是下載惡意檔案的機率就會比較高。

多留意詐騙與身份冒用

- 當駭客搜集了我們的個資以後，可能會**利用這些資訊來冒用**我們的身份去**詐騙別人**，或是反過來用這些資訊**假裝成銀行或是政府機關來詐騙你**。

從錯誤中學習

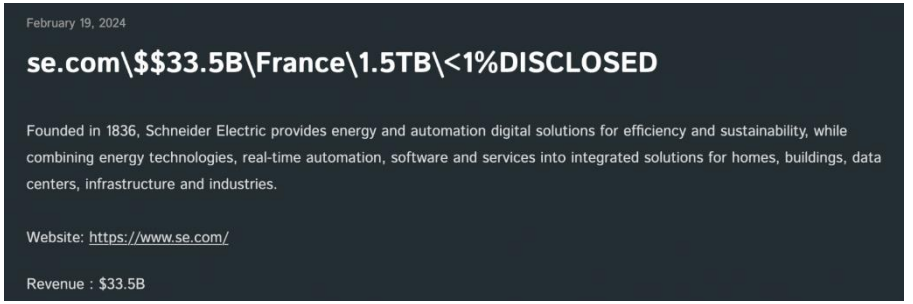
常見的駭客攻擊手法大概都很雷同，如果我們能夠**清楚了解為什麼帳號被駭**，**防護是否足夠**，或是**對釣魚陷阱的意識，補強**做的不足夠的地方，就可以**避免**自己在未來遇到類似的攻擊手法時再次中招。

KPMG

近期資安暨個資案例 2
勒索軟體攻擊

施耐德電機近日遭 Cactus 勒索軟體攻擊

- Cactus勒索軟體攻擊鎖定施耐德電機的永續發展業務部門，影響到施耐德電機的部分資源顧問雲端平台，被盜資訊包含**客戶用電、工業控制和自動化系統以及環境和能源法規合規性的敏感資訊**。由於永續發展業務是一個獨立作業單位，與施耐德電機網路基礎設施隔離，因此集團內沒有其他單位受到影響。
- 一旦威脅行為者**獲得網路存取權限**，Cactus會**滲透到其他系統，同時竊取伺服器上的公司資料**。在竊取資料並獲得網路管理權限後，威脅行為者會對檔案進行加密並留下勒索資訊。 Cactus也會進行**雙重勒索攻擊**，即他們要求贖金以獲得文件解密器並承諾銷毀且不洩露被盜資料。那些不支付贖金的公司，Cactus會在資料外洩網站上洩露所竊取的資料。



資料來源：資安人 2024/02/01

中國勒索軟體Crazyhunter 入侵我國馬偕醫院

馬偕紀念醫院遭駭客「Crazyhunter」以勒索病毒攻擊，透過加密醫院個人檔案，讓病患資料無法開啟，電腦病毒陸續蔓延，導致醫院門診看急診系統500多臺電腦當機，並留言恐嚇馬偕醫院交付贖金，否則網路論壇上揭露及販售個人資料。

攻擊手法

- 攻擊者在入侵過程中會從AD管道下手，透過弱密碼嘗試取得帳號權限，進而透過GPO派送方式發動大範圍勒索加密攻擊。
- H-ISAC的公告內容指出，目前已知攻擊路徑為AD主機並派送惡意程式，惡意程式名稱如下：(1)bb.exe，(2)crazyhunter.exe，(3)crazyhunter.sys，(4)zam64.sys，(5)go3.exe，(6)go

資料來源：iThome 2025-02-12

新興勒索軟體Anubis抹除檔案內容進行施壓

- 趨勢科技揭露勒索軟體攻擊態勢出現重大改變，他們看到名為Anubis的新興勒索軟體結合了**資料抹除（Wiper）**功能，使得受害組織**無法藉由竊密金鑰復原內容**，受害組織承受更大的壓力。
- Anubis使用新經營模式，分成三種類型的附屬團體分別負責不同階段的攻擊流程，並以利潤拆分的方式合作。
  1. **勒索軟體攻擊執行者：**負責實際部署與執行勒索軟體攻擊
  2. **勒索談判與金錢勒取者：**負責迫使受害者支付贖金以換取資料或系統的恢復
  3. **初始入侵管道提供者：**負責挖掘並販售企業的初始入侵點（如弱密碼、漏洞、釣魚等）

Anubis = 加密 + 抹除資料

遭到勒索軟體攻擊的檔案雖然看似並未刪除，副檔名也未被更動，但檔案內容皆完全被清除，大小變成0 KB。

資料來源：iThome 2025-06-17

麒麟Qilin勒索軟體再度來襲：一週內兩起攻擊台灣

麒麟（Qilin）勒索軟體是一種高度組織化、策略性強的**勒索即服務（RaaS, Ransomware-as-a-Service）攻擊工具**，自 2022 年底活躍至今，對台灣與全球企業造成重大威脅，最新兩起攻擊事件如下：

1. **2025/5/29**：麒麟公布入侵台灣跨國企業集團旗下加拿大飯店，洩露16張截圖，包含台灣嘉義關係企業的帳務系統、銀行資訊等，顯示高度橫向滲透能力。
2. **2025/5/30**：再公布攻擊台北市某汽車零件製造大廠，該公司在雲林、台中與中國上海設有工廠，並洩露17張截圖。

資料來源：iThome 2025-06-04

什麼是勒索病毒？

勒索病毒近年越頻繁地發生於政府、組織中，造成的損失金額也漸增

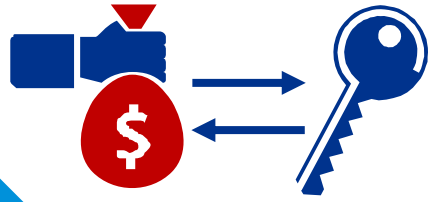
1

勒索病毒加密
裝置中的檔案

2

造成其他檔案
軟體無法使用

3



勒索贖金
以換取解密

但是：即使支付贖金，仍然**無法確保**駭客會解密該檔案，且無法確保未來系統或資料不會再被駭入。

→ 故：國際上，幾乎所有資安組織都**不建議**支付贖金。

勒索病毒特色

事先潛伏、伺機而動

- 駭客可能在數月前透過員工個人電腦、網頁或DB伺服器，入侵公司內部網路並開始刺探與潛伏，竊取特權帳號後侵入網域控制伺服器(AD)。
- 竄改群組原則派送具惡意行為的工作排程，執行排程時將駭客預埋在內部伺服器中的勒索軟體下載至記憶體中執行。

勒索病毒攻擊手法

第一階段

- 入侵員工電腦、伺服器
- 潛伏於公司內網

第二階段

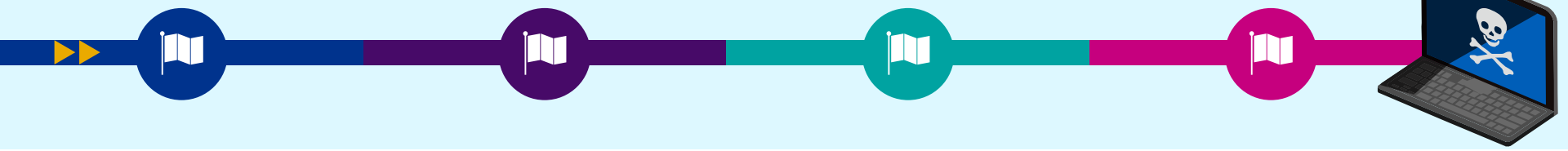
- 竊取特權帳號
- 侵入網域控制伺服器

第三階段

竄改排程派送具惡意行為的工作排程

第四階段

遭加密顯示勒索訊息/電郵，要求贖金以取回檔案



如何防範勒索病毒？

KPMG建議

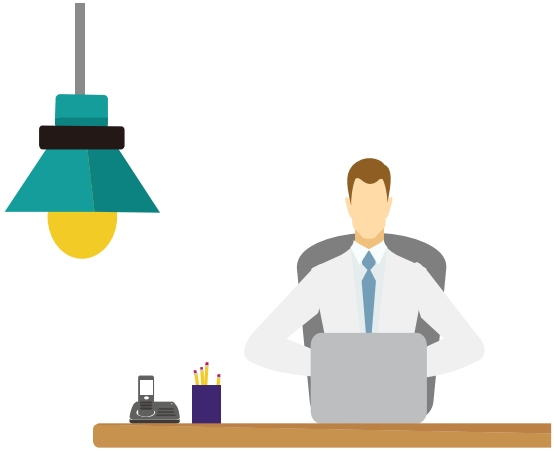
- ✓ 不明郵件**請勿**開啟，不輕易相信中獎、優惠、折扣、免費等不實訊息。
- ✓ 如對來信有疑問，需先**連絡寄件人**確認郵件和附件來源。
- ✓ 不點選可疑的**網路連結**或下載可疑的**檔案**，連接USB時需先確保內容是可信任的來源。
- ✓ 公務用信箱**請勿**用於**註冊外部網路服務**，避免個資的洩漏，以防範可能的社交工程攻擊。
- ✓ 定期進行**弱點掃描**，確認是否存在已知漏洞並進行修補。
- ✓ 配合資訊單位**定期更新**病毒定義檔及電腦作業系統安全性更新。
- ✓ 重要案件、檔案**請務必**依規定進行**歸檔**。
- ✓ 資料備份，定期進行**備份還原演練**確保資料有效性。
- ✓ 平常或發生重大網路攻擊事件之後，應重新檢視網路安全**應變操作計畫**及**災害復原計畫**。
- ✓ 應嚴加限制**核心網路**或**重要營運系統**透過外部網際網路瀏覽器的存取。
- ✓ 確實**保護AD管理者**，加強密碼強度、管制登入位置。
- ✓ 確認所有**防火牆設備**的規則管理、嚴格限制外部遠端桌面協定（RDP）相關設定。

KPMG

近期資安暨個資案例 3
木馬程式攻擊

【四大銀行客戶員工資料先後外洩】木馬程式Infostealer防不勝防

- 木馬程式Infostealer近期再度針對**澳洲四大銀行**實施攻擊，共有**31000筆客戶資料及100名員工的登入資訊**遭到外洩，可能導致駭客使用員工帳號成功存取系統資料，造成更進一步地破壞。
- 該木馬程式透過**受感染的員工個人設備**存取工作資源，進入系統後即可安裝勒索軟體並取得大量用戶資料，使得公司面對敲詐勒索、商業Email外洩及智財權竊盜...等犯罪行為。被竊資料亦可能包括使用者名稱和密碼、信用卡詳細資料、加密貨幣錢包...等，導致使用者面臨詐騙損失之風險。



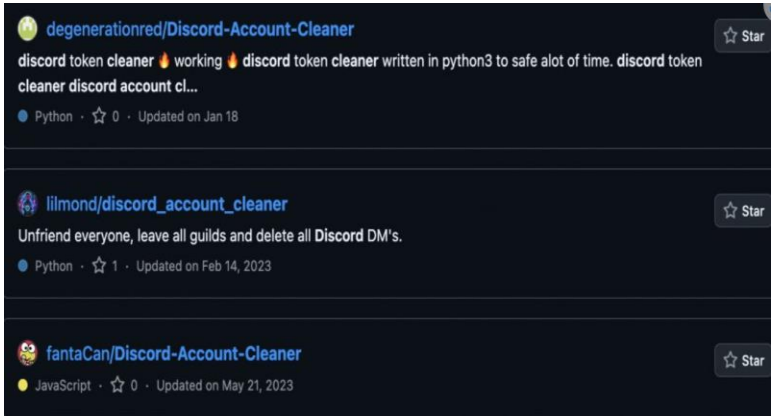
資料來源：SBS中文 2025/05/06

GitHub出現67個木馬專案，Banana Squad 攻擊軟體供應鏈竊取開發者資料

- 資安公司 ReversingLabs 發現，駭客組織 Banana Squad 在 GitHub 上建立 67 個**仿冒熱門 Python 專案的惡意倉庫**，目的是竊取開發者的敏感資料。
- **攻擊目標與影響：**
  1. 鎖定開發者與 IT 專業人士。
  2. 竊取系統資訊、應用程式資料、瀏覽器紀錄、加密貨幣等。
  3. 2023 年類似攻擊在 PyPI、NPM 等平台已累積 超過 7 萬次下載。
  4. GitHub 已下架 67 個惡意專案，但由於開源專案易於複製，實際難以全面掌握

攻擊手法

- 冒用熱門 Python 專案名稱，吸引開發者下載。
- 惡意程式碼藏於原始碼中，利用大量空白字符將木馬隱藏在螢幕右側，降低被發現機率。
- README 檔案混淆視聽，常出現亂數字串，模仿合法專案說明。



資料來源：iThome 2025-06-24

駭客假冒 LINE 電腦版進行木馬攻擊

趨勢科技發現，近期有駭客集團將木馬程式**偽裝成「LINE 電腦版」**應用程式，透過搜尋引擎誘導使用者下載，進而植入惡意程式。駭客建立與真實網站極為相似之LINE軟體下載網站，吸引民眾於假冒之網站下載軟體。用戶遭詐下載軟體後，木馬程式即被安裝於電腦內，導致**裝置被控制、勒索或個資外洩**之風險。

防範建議

- 確認網址來源是否為官方網站，僅從 LINE 官方網站或可信平台下載應用程式
- 使用專業資安工具，防範來自簡訊、電話等詐騙。
- 確保資安軟體與病毒碼為最新版本，以即時偵測與阻擋威脅。

資料來源：經濟日報 2025/04/11、台視 2025/04/12

ToxicPanda 偽裝 Chrome 木馬病毒攻擊

ToxicPanda是一款新型木馬病毒，源自於舊有的惡意軟體家族TgToxic，專門用於金融詐騙攻擊，專門針對銀行帳戶與金融應用進行詐騙攻擊。該病毒具備高度隱蔽性，能偽裝成 Google Chrome等熱門應用程式，讓使用者在不知情的情況下輸入敏感資料，導致資金被盜。

該木馬能夠**攔截用戶的一次性密碼（OTP）**，讓攻擊者濫用Android的安全和可存取性服務，以獲得進階功能和更高的權限。更具威脅的一點是，ToxicPanda允許攻擊者啟動**遠端控制**，直接訪問受害者的裝置執行各種操作，例如**查看個人數據、移轉資金**等。

建議措施

- 避免側載應用程式：不要從**非官方或第三方網站下載應用程式**，這些來源可能缺乏安全性檢查，容易挾帶惡意軟體。建議只在Google Play Store、Apple App Store等官方應用商店下載應用程式，降低惡意程式入侵風險。
- 定期更新裝置：確保設備的作業系統與應用程式保持在**最新版本**，以修補已知的安全漏洞。
- 密切關注銀行帳戶的活動，及早發現任何可疑交易。

資料來源： Yahoo 2024-11-13

瞄準 iPhone 用戶銀行帳戶，木馬程式 GoldDigger 出沒

- Android 木馬程式 GoldDigger 近期再度出現變種名為 GoldPickaxe，更容易竊取受害者銀行帳號內的存款，同時這款木馬程式現在也**針對 iOS 系統設計出新版本**。
- GoldPickaxe 木馬程式主要是針對普通用戶而來，一旦安裝在 iPhone 或 Android 手機，就能夠**竊取臉部辨識資料、私密文件和攔截訊息**，導致攻擊者能**利用 AI 深度偽造臉部識別數據**，冒充受害者進入銀行帳號，導致能輕鬆從銀行和其他金融應用程式中竊取受害者存款。

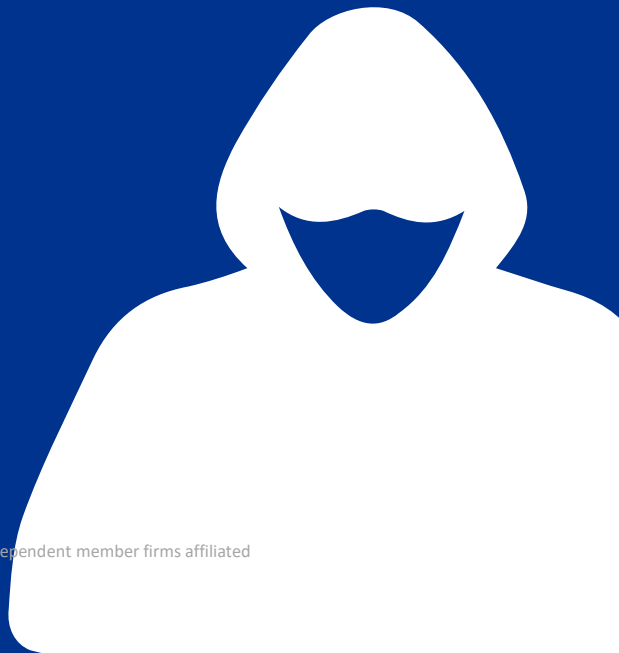
資料來源：資安快報2024/02/16

什麼是木馬程式？

- 簡單來說就是惡意程式。但是和病毒或蠕蟲不同，木馬並不進行自我複製，主要目的就是窺視每台電腦中的機密，例如信用卡卡號、身分證字號、銀行帳號、各式帳號密碼等。
- 原則上它只是一種遠端管理工具，為了能夠順利入侵你的電腦，首先必須把一小程式植入你的電腦，再透過這個程式進行資料竊取，本身不帶傷害性，也沒有感染力，所以不能稱之為病毒。

潛伏隱匿，操控竊密

- 不需要本身的使用者準許就可獲得電腦的使用權。
- 程式體積十分微小，執行時不會佔用太多資源。
- 執行時很難停止它的活動。
- 執行時不會在系統中顯示出來。
- 一次執行後，就會自動登錄在系統啟動區，之後每次在 Windows 載入時自動執行。
- 一次執行後，就會自動變更檔名，甚至隱形。
- 做到連本身使用者都無法執行的動作。



如何防範木馬程式？(1/2)

KPMG建議

✓ **不要執行任何來歷不明的軟體**
很多木馬程式都是透過綁在其他的軟體中來傳播的，一旦運行了這個被綁定的軟體就會被感染，因此在下載軟體的時候需要特別注意。在軟體安裝之前一定要用**防毒軟體檢查**一下，建議用專門殺木馬的軟體來進行檢查，確定無毒後再使用。

✓ **不要隨意打開郵件附件**
現在絕大部份木馬程式都是透過**郵件來傳遞**的，而且有的還會連環擴散，連累其它電腦，因此對郵件附件的運行尤其需要注意。

✓ **將檔案總管設定成"始終顯示副檔名"**
將Windows檔案總管設定成**始終顯示副檔名**，一些文件副檔名vbs、shs、pif的文件多為木馬程式的特徵，如果碰到這些可疑的文件副檔名時就應該要特別注意。

如何防範木馬程式？(2/2)

KPMG建議

✓ **執行反木馬即時監控軟體**

木馬防範重要的一點就是在上網時最好執行**反木馬即時監控軟體**，The Cleaner等軟體一般都能即時顯示當前所有執行中的程式並有詳細的描述資訊。此外加上一些專業的最新的防毒軟體、個人防火牆等進行監控就可以放心了。

✓ **經常更新系統**

很多木馬都是透過系統漏洞來進行攻擊的，微軟公司發現這些漏洞之後都會在第一時間內發佈更新檔，只要執行**Windows Update更新**系統就是一種最好的木馬防範辦法。

KPMG

社交工程認知與宣導

KPMG

何謂社交工程？

企業最大資安隱憂竟然是人?! 社交工程是什麼?

社交工程常見方法

佯裝資訊人員：利用電話佯裝資訊人員，騙取帳號及通行碼。

假冒委外廠商：及通行碼。
偽裝委外廠商之維護人員或上級單位人員，乘機騙取帳號

偽造釣魚網站：利用電子郵件誘騙使用者登入偽裝之網站以騙取帳號及通行碼，如網路釣魚。

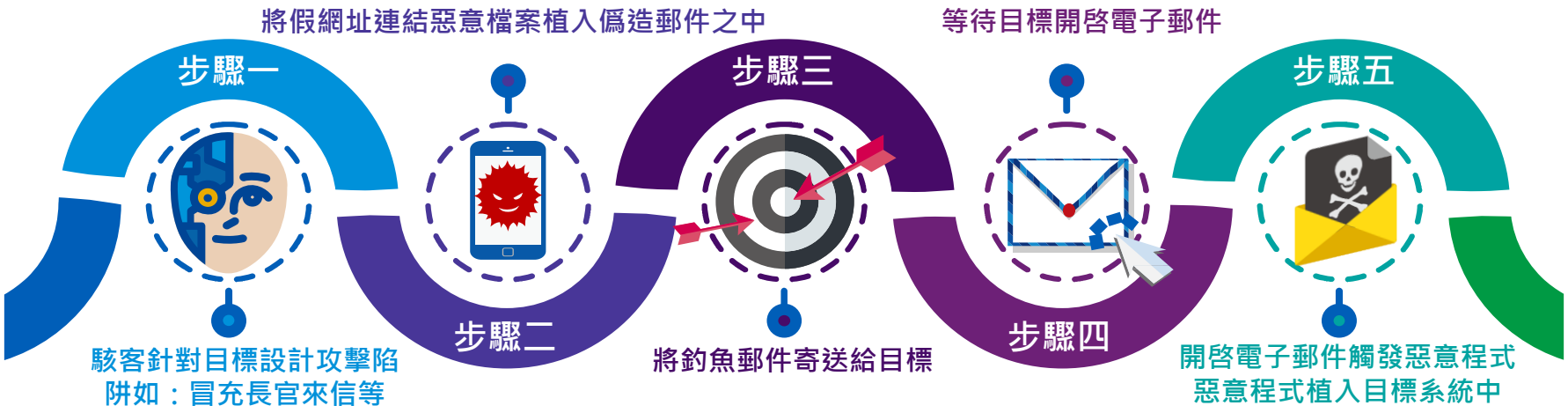
惡意程式附件：利用電子郵件誘騙使用者開啟檔案、圖片，以植入惡意程式、暗中蒐集機敏性資料。

冒充軟體更新：誘騙使用者下載，如偽裝的修補程式、P2P下載軟體、工具軟體等，乘機植入惡意程式。

駭客想要盜取的資訊

電子郵件社交工程模式

常見攻擊模式



KPMG

社交工程案例分析

個資外洩→網路釣魚？！

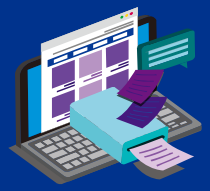
個資外洩與網路釣魚之間的關係

兩者之間的關聯性？

- **網路釣魚**可以**引起個資外洩**，當人們被騙時通常會透露他們的個人資訊。
- **個資外洩**可為駭客進行**網路釣魚**時提供更多的目標資訊，使詐騙更具說服力。

KPMG觀點

1. 提高對網路釣魚社交工程技巧的認識。
2. 不要隨便點擊**不明連結**或**下載附件**。
3. 確保**個人信息**的**儲存**和**使用**符合**安全標準**。
4. 使用**強密碼**並**定期更換**。



網購女大生遭「賣貨便假客服」詐騙損失27萬

一名女子在Threads發文分享，為了買450元毛巾結果損失27萬，大學學費、出書的錢全被騙光，她曬出對話截圖，只見對方自稱是「賣貨便線上客服」，以帳號有安全疑慮為由，要求她提供姓名、電話、銀行帳號等個人資料，接著再騙她填寫餘額數字進行驗證，等反應過來錢已經沒了。

資料來源： TVBS 2025-07-25

購物網站？偽冒網站？社交工程？

兩者之間的關聯性？

- **社交工程**常被用來對購物網站的**用戶進行攻擊**，例如，詐騙者可能會偽裝成網站的客服人員，試圖獲取用戶的個人和付款資訊。
- 詐騙者也可能設立**偽冒網站**，這些網站看起來和真實的購物網站一模一樣，但其實是用來**收集用戶資訊**的。

KPMG觀點

1. 提高對社交工程技巧的認識，並學習如何**識別可能的欺詐**。
2. 不要隨便點擊**電子郵件中的連結**，特別是那些看起來像購物網站的連結。
3. 確保您的**付款資訊**是在**加密和安全**的連接中傳輸的。

微軟重大漏洞：SharePoint 遭零時差攻擊，近百組織受害

微軟 SharePoint 伺服器近日遭駭客利用「零時差漏洞（zero-day）」發動大規模網路間諜行動。駭客可全面存取 SharePoint 檔案系統，甚至連帶影響 Microsoft Teams、OneDrive 等服務。受害對象近百個組織，包括美國與德國的政府機構、企業、銀行、醫療機構等。

資料來源： Yahoo 新聞 2025-07-22

社交工程與零時差攻擊之間的關係

兩者之間的關聯性？

- 可**利用社交工程**進行**零時差攻擊**，例如：攻擊者可能會利用**社交工程**技巧**誘使受害者下載有害的軟體**，這種軟體利用未知的漏洞來入侵系統。
- 社交工程和零時差攻擊經常一起使用，使攻擊更加有效。

零時差攻擊是什麼？

是指攻擊者在**軟體**或**系統漏洞被公開或補丁發佈之前就開始進行攻擊**。

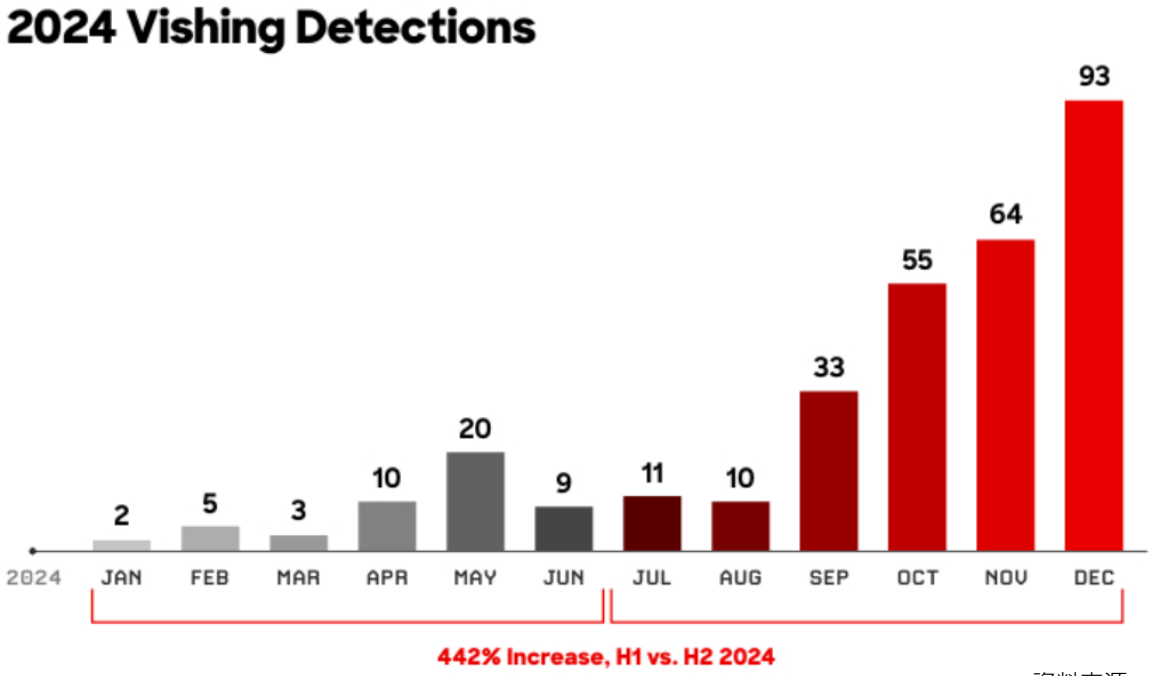
這種攻擊通常**很難防範**，因為**沒有人知道這種漏洞的存在直到攻擊發生**。

KPMG觀點

1. 保持軟體和系統的**最新版本**，即使這不能保護你免受零時差攻擊，但它可以**減少其他已知漏洞的風險**。
2. 提高對社交工程技巧的認識，不要隨便點擊**不明連結**或**下載未知的檔案**。
3. 使用網路安全工具，如防火牆、防病毒軟體等。

2025社交工程攻擊新趨勢！語音網釣、AI偽冒真實攻擊大增

資安業者Crowdstrike發布2025全球威脅報告，當中揭露了語音網釣的最新變化，以2024上半年而言，每個月最多僅發現20起語音網釣活動，但下半年、尤其是第四季，數量動輒達到50起以上，比上半年增加了4.42倍。



資料來源： iThome 2025-07-11

山形鐵道公司遭自動語音網釣詐騙近億日元，企業網路銀行帳密是攻擊者下手目標

日本山形鐵道在2025年3月，傳出遭假冒山形銀行的語音網釣（Vishing）詐騙，**損失約1億日元（約2,000萬元）**，更令人警惕的是，這類攻擊的鎖定對象與典型的商業電子郵件詐騙（BEC）如出一轍，直接**鎖定掌管企業網路銀行的公司財務人員**而來。

1. **偽冒銀行語音來電：**詐騙者使用自動語音假冒山形銀行，聲稱企業網銀（Net EB）帳戶需在2小時內更新，否則將停用。
2. **轉接至假客服人員：**受害者依語音指示按鍵後，電話轉接至冒充銀行職員的詐騙者。
3. **索取公司電子郵件並發送釣魚郵件：**詐騙者要求提供聯絡用電子郵件，並寄送含釣魚網站連結的郵件，誘導受害者填寫公司與網銀帳戶資訊。
4. **再次來電騙取驗證資料：**受害者填完表單後，詐騙者再次來電，引導操作網銀或OTP設備，取得驗證資料。
5. **成功盜轉企業資金：**詐騙者利用取得的帳號密碼與驗證資訊，非法轉走企業銀行帳戶資金。

資料來源： iThome 2025-07-11

社交工程-語音釣魚(Vishing)

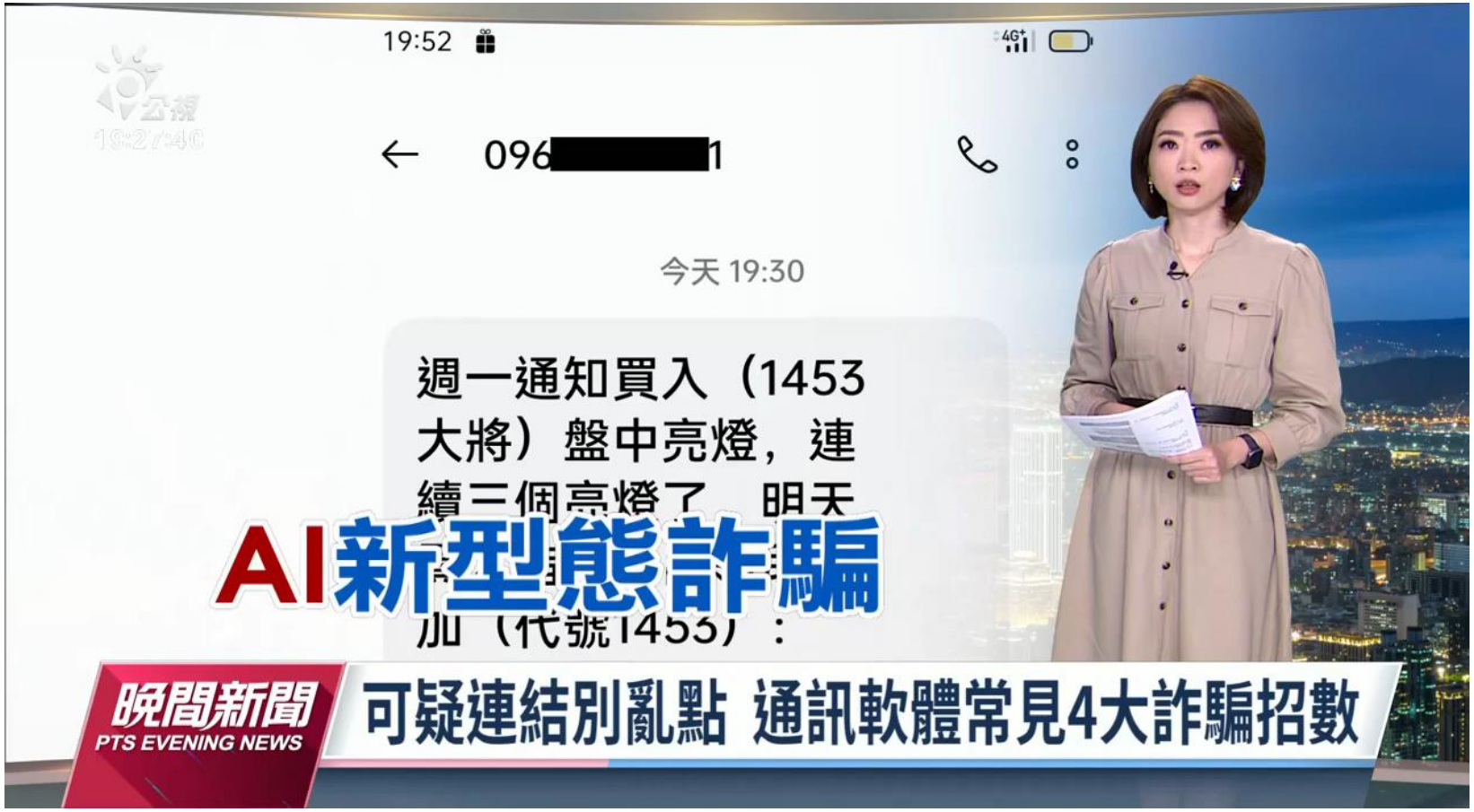
何謂語音釣魚(Vishing)？

- 是一種**社交工程詐騙**，攻擊者會**偽裝**成他人來打電話給受害者，目的是為了**騙取個人資料或金錢**。
- 語音釣魚跟社交工程息息相關，通常是利用**受害者心理**來說服他們採取行動。語音釣魚詐騙者會用**威脅**或**獎勵**的方式來讓受害者覺得自己必須服從。受害者經常會收到**威脅性**的**語音郵件/電話**，出現像是**法庭案件**或**凍結帳戶**等內容。

KPMG觀點

1. 提高對社交工程技巧的認識，特別是如何識別**語音釣魚攻擊**。
2. 不要在接到來電要求提供**個人**或**財務信息**時**直接給出**，特別是當通話裡帶有**強烈的急迫感**。
3. 當收到**不明來電**或是**未知來電且開頭有+號**時，可以直接掛斷電話。

通訊軟體與社交工程：四大詐騙招數與防範策略



如何預防新型態通訊軟體詐騙？

新型態的通訊軟體詐騙介紹

- 根據調查，通訊軟體去年就偵測到1.4萬的可疑連結
- 描述**假投資以及其他新型態的詐騙**，包括**LINE輔助認證**和**Google表單詐騙**

社交工程的技巧？

- 使用社交工程技巧進行這些詐騙，如**建立信任、利用恐慌感**等
- **AI科技**的發展如何可能使**詐騙更為狡猾**，並增加了資安與網路犯罪的風險

KPMG觀點

1. 提醒大眾對任何在通訊軟體中接收到的**可疑連結保持警惕**
2. 建議進行反社交工程的訓練和教育，以提升對**這些詐騙手法的識別能力**
3. 強調在進行任何形式的金錢交易或資訊分享之前，**確認對方的身份與可信度**

利用員工的社群網站 、電子郵件入侵公司?

KPMG

如何防範社交工程？

如何防範社交工程?

Google

How to avoid a social engineering attack

如何避免社交工程攻擊

如何防範社交工程？(1/2)

KPMG建議

避免人性弱點遭利用：

- ✓ 提昇自我資安認知與警覺性
- ✓ 重要資料或密碼輸入時，應注意是否有旁人窺視
- ✓ 討論業務機密應注意場合
- ✓ 透過網路或電話溝通時，應確認對方身份
- ✓ 使用者帳號或密碼不可洩漏給任何人

平時電腦使用習慣：

- ✓ 安裝正版防毒軟體並定期執行更新及掃毒
- ✓ 定期更新作業系統和應用程式漏洞
- ✓ 定期更換密碼，且強度要夠

如何防範社交工程？(2/2)

KPMG建議

電子郵件防禦注意事項：

- ✓ 非公務業務相關不明來源與可疑之電子郵件請直接刪除，勿開啟、勿轉寄
- ✓ 不輕易點選、下載或回傳電子郵件內的連結
- ✓ 取消郵件預覽功能
- ✓ 不隨意開啟附件(附加檔案件及資料)
- ✓ 確認寄信人與主旨間的關係
- ✓ 非經查證，不要直接點選郵件中的超連結 ，詳細檢視網址是否正確(可將常用的網址加入我的最愛)
- ✓ 善用密件收件人

新興議題分享

KPMG

新興議題案例：
生成式AI引發應用危機

美國新住房騙局 用AI冒充房仲、貸款方詐騙 甚至不需高級技能就能騙

詐騙者使用生成式人工智慧(AI)，冒充房地產仲介、貸款人或房屋銷售過程可能涉及的各方，模仿他們的電子郵件寫作風格或語音郵件聲音，誘導毫無戒心的收件者將資金匯入詐騙者帳戶。

1. 詐騙者可以**利用侵入帳戶和在網路上冒充房地產專業人士**，獲取交易詳細信息，了解詐騙所需資訊。他們還可以使用房地產資料庫和對外公開的上市訊息，在詐騙電郵中添加有說服力的細節。
2. ChatGPT等免費AI程式可以**讓詐騙者編寫出更好的網路釣魚電郵**，誘騙收件者點擊連結或附件訊息，「過去假冒失敗的不良演技問題變小了，他們並不需要任何高級技能就能行騙」。

KPMG觀點

- 面對新型態的威脅，傳統的資安防禦措施可能不足。公司需要強化如零信任架構、跨部門協作的快速響應機制，以及針對生成式AI的專屬防護措施。
- 政府也需協助提升法規與道德規範，針對生成式AI的應用需要更嚴格的法律監管與行業道德標準，特別是在金融、選舉等敏感領域，以減少濫用的可能性。

資料來源：聯合新聞網 2024.12.16

AI詐騙 財經名人遭冒充誆「選股成功率95%」

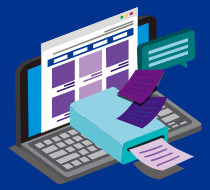
近期詐騙集團「假投資」出現知名股票資訊公司背景的詐騙網路影像，號稱可以提供「成功率百分之95」選股工具，製作精良幾可亂真，民眾一不小心就上鉤。刑事局預防科今天表示，這些盜用股票資訊公司背景、素人假冒的財經專家權威都是AI人工智慧的產物，民眾務必小心不要上當。

1. 生成式人工智慧（Generative AI）迅速發展，詐騙集團已經開始將這項技術運用於提升**投放詐騙假廣告能力**。由於生成式AI操作簡單，許多基礎模型甚至**可免費或低價取得**，詐騙集團能夠快速、低成本製作大量且日趨精密的詐騙內容，例如**網路釣魚信件、假親友電話、假冒名人影音**都深偽更真。
2. AI生成式影音爆發後，**全球串流式影音詐騙廣告增加6成**，特別是YouTube與Meta的Reels短影音，已經出現盜用知名股票資訊公司背景，以素人假冒財經專家權威揭露新的財經消息，引導民眾加入封閉式社群媒體LINE或Telegram，再誘使被害人加入詐騙投資APP平臺，讓被害人活在深偽包圍的網路環境。

KPMG觀點

呼籲社會大眾於網路社群媒體所看到的財經資訊分享、股票投資秘笈大公開等廣告及貼文，都不可輕易相信，特別是經由網路上提供的投資APP，如同陷阱精密度提升的詐欺捕獸夾，無情吞噬民眾財產。

資料來源：三立新聞網 2024.11.16



AI詐騙橫行黑色星期五購物潮

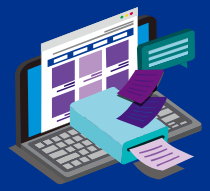
美國聯邦貿易委員會（Federal Trade Commission，FTC）統計顯示，自2021年以來，約四分之一的詐騙起源於社群媒體廣告，利用廣告目標受眾技術鎖定潛在受害者。同時，假冒物流公司傳送送貨通知、索取個資的手法也屢見不鮮。更有駭客利用搜尋引擎廣告吸引消費者點擊，將其導向虛假的購物網站，進一步套取個人資料與金錢。

1. 根據Barclays的調查，假冒Amazon或Costco等零售商的**促銷郵件**是最常見的詐騙形式之一。
2. **深偽技術（DeepFaker）**更進一步提升詐騙的誤導性，駭客能製作出極為逼真的名人代言影像，吸引受害者上當。雖然有調查顯示，59%的受訪者認為自己能辨識深偽技術生成的內容，但事實上，駭客利用這些技術大規模複製網站、生成虛假廣告或優惠訊息，降低人們的警覺心。

KPMG觀點

- 建議消費者啟用信用卡支付通知功能，對每筆交易進行即時通知，並啟用金融應用中的雙因素驗證（2FA），即使卡號被盜也難以進一步濫用。
- 針對企業，建議大型零售商和品牌應採用數位水印或內容簽章技術，為官方的促銷活動和網站進行驗證，並強化對品牌名稱和標誌的監控，利用工具自動檢測網路上的假冒網站或內容。

資料來源：三立新聞網 2024.11.22



網路交友平台透過生成式人工智慧進行詐騙

一名英國女性在網絡交友平台上認識一位聲稱為美國陸軍上校的男子。詐騙者利用生成式人工智慧（AI）技術，製作深偽影像和語音，塑造可信的虛假身份。經過多次交流，受害者逐漸建立信任，並被對方誘導匯款，最終損失20,000英鎊。

1. 詐騙者利用**生成式AI的深偽技術偽造虛假身份**。並透過長期交流與心理操作建立受害者信任，進而誘導金錢交易。
2. 根據英國支付系統監管機構的數據，2023年此類騙局被盜4.597億英鎊。此前，電信公司 O2 最近發佈了他們的 AI 詐騙打擊機器人大軍，這些機器人旨在模仿老年人——常見的詐騙目標——並浪費欺詐者的時間。

KPMG觀點

- 民眾個人在交友過程中，對於聲稱擁有特殊身份（如軍官、外交官等）的陌生人須保持高度懷疑，特別是當對方提到金錢或物品交易時。
- 生成式AI為一大新趨勢，延伸至企業面，公司也須針對Deepfake與生成式AI詐騙的專屬培訓，教導員工如何辨別虛假內容，尤其是從事金融、客服等高風險職位的員工

資料來源：Irish Sun 2024.11.19

AI時代下的資安危機 / 如何防範駭客攻擊
專家：資安意識最重要

國內企業近年發生駭客攻擊事件頻傳，甚至還出現將民眾個資洩漏、遭主管機關重罰的案例。專家建議，企業除了落實數位系統管理、精進漏洞掃描及修補等技術外，提升「資安意識」將是重中之重。

資安防範三原則：管理、技術、意識

在管理方面，例如資安相關的ISO27規範，一定要合規，落實數位系統相關管理；其次靠技術如精進漏洞掃描及修補來把關，最後也是最重要的就是提升員工資安意識，釣魚郵件不要點等教育宣導。

眼見不能為憑 民眾須提升警覺性

資安專家呼籲，任何不明來源的圖片、影像、音訊等皆可能是詐騙集團透過生成式AI技術偽造而成，民眾對任何網路上的訊息**均應檢查來源、再三查證**。

法規日趨嚴謹 企業資安投入迫在眉睫

在網路環境越趨複雜的情況下，推動零信任(Zero Trust)架構、也就是任何交易、個體與身分在獲得信任並持續維持信任之前，全都不可信任，和過往認為網路在被發現遭到入侵之前是安全的的觀念完全不同。

KPMG觀點

威脅情資也能夠提升大眾的資安意識，密切關注新興資安威脅與發展趨勢，例如生成式AI帶來的新型攻擊手法和風險，亦或是與資安機構、廠商建立夥伴關係，及拾取的資安情報，皆有助於企業防範駭客威脅。

資料來源： iThome 2024.03.14

AI時代下的資安危機 / 文字、聲音、影像都能造假 連駭客都進階了

生成式AI可幫忙生成文章、圖像、藝術創作、程式語言等，為工作大大加分，就在讓民眾越來越依賴的同時，竟也成為助長網路犯罪的工具。勒索軟體和黑帽駭客激進主義持續猖獗，2023年發生多起大規模攻擊，可觀察到網路犯罪份子不斷升級手段和工具，這些「進化」可能都歸功於生成式AI。

生成式AI 資安的雙面刃

- 生成式AI可以幫助資訊人員加速工作進度，對黑帽駭客當然也有同樣效果，可以幫助他們開發惡意程式，以及內容的產出，像是寫出很誘人的釣魚郵件，甚至創造假訊息。

全球勒索軟體攻擊上升 零售及批發行業成重要目標

- 零售及批發行業年增率大幅暴增至22%，Check Point分析，零售和批發企業通常會處理來自大量客戶的財務資料，如信用卡、財力等個資，且他們通常涉及眾多供應商和第三方服務提供者，對黑帽駭客充滿吸引力。
- 些產業正開始數位轉型，嚴重依賴線上交易，與大型企業相比，小型零售商和批發商可能沒有強大的網路安全防禦資源，這些數位足跡都為網路攻擊者提供了更多的入口點。

駭客的新模式 RaaS崛起

- 勒索軟體的演進，攻擊者已改變策略，透過零日漏洞、也就是當漏洞被發現，而軟體開發商尚未發布修補程式時，以更強手法攻擊
- 針對邊緣裝置、如手機、遊戲機、安全攝影機的攻擊持續增加，凸顯出所有網路元件都可能需要安全措施。
- 國家支持的駭客激進主義不斷升級，與地緣政治衝突相關的網路攻擊顯著提升。

資料來源： 中廣 2024.03.14

AI老手如何防護生成式AI Amazon安全長首揭露

Amazon的安全長 Steve Schmidt 提到了在AI領域中，通常企業會將AI安全團隊視為“守門員”，由專家審查並確保安全。然而，這種方式可能成為開發流程的瓶頸，拖慢創新速度。因此，亞馬遜選擇讓安全團隊成為“助攻員”，協助開發人員建立安全防護解決方案，包括防護工具、檢驗工具和防護機制。這與亞馬遜倡導的「分散式安全」理念一致，將安全實踐分散到各個部門。

此外，亞馬遜也開發了生成式AI安全需求評估框架，名為「Generative Artificial Intelligence Scope Matrix」。此框架可協助開發團隊評估專案範圍和安全防護方面。

亞馬遜的AI安全團隊採取了一系列措施來加強生成式AI的安全：

1 生成式AI安全標準

確保處理機密資料、偵測模型和AI應用服務的安全性。

2 威脅模型分析指南

透過系統性方法分析潛在威脅，設計緩解措施，並確定優先級，以確保最大限度地發揮有限資源的安全效果。

3 提供測試工具：

根據威脅模型分析結果，開發相對應的測試工具，幫助開發人員檢驗生成式人工智慧應用程式的安全性。

4 持續性安全檢驗

生成式AI的安全檢驗沒有完成的一天，現在更需要改變成持續性檢驗。亞馬遜的AI安全團隊開發了防護機制工具，可以評估使用者輸入和模型輸出的內容，並過濾有害內容、提示攻擊或包含敏感個資的資料。

AI老手如何防護生成式AI Amazon安全長首揭露

企業在推出生成式人工智慧應用前應重視以下四大安全守則：

在訓練人工智慧模型時，要清楚掌握資料來源、儲存位置、存取權限以及使用目的。檢視日誌檔案以了解資料實際的使用情況。

在檢索增強生成（RAG）領域中，確保人工智慧應用提供正確的上下文，並且只能存取經過使用者授權的資料。

根據人工智慧應用的特性，定期或持續地使用特別設計的提示來測試模型，主動偵測潛在的注入攻擊或資料外洩問題。

為了過濾不適當的術語或主題，任何AI應用都需要防護機制，以根據使用者的性質進行過濾。

AI老手如何防護生成式AI Amazon安全長首揭露 | iThome

KPMG

2024年資安趨勢回顧與2025資安趨勢分析

2025年九大網路安全趨勢概覽

Check Point發布了2025年九大網路安全趨勢預測，歸納如下：

生成式AI多樣化

攻擊模式日益精細，
增加偵測難度

勒索軟體影響供應鏈

擴展至供應鏈合作夥伴

AI 使用風險

無意的資料外洩風險增大

量子計算威脅

傳統加密技術面臨量子計算挑戰

AI 驅動 SOC 助手

加強威脅偵測和應對效率

深度偽造詐騙

加劇金融與個人資料安全隱患

CIO 和 CISO 角色融合

資安與 IT 策略更緊密協作

雲端安全平台主導

多雲架構安全防護成為關鍵

物聯網攻擊面擴展

IoT 設備安全需求日益增加

AI 驅動攻擊日益增多

資安威脅九大面向

- 生成式AI多樣化
- 量子計算威脅
- CIO 和 CISO 角色融合
- 勒索軟體影響供應鏈
- AI 驅動 SOC 助手
- 雲端安全平台主導
- AI 使用風險
- 深度偽造詐騙
- 物聯網攻擊面擴展

2025 年 AI 將成為**網路犯罪**的主要幫兇。攻擊者將利用 AI 技術發起高度客製化的**網路釣魚攻擊**，以及生成能夠從即時資料中學習、躲避偵測的**自適應惡意軟體（adaptive malware）**。

小型駭客組織也可**利用 AI 工具發起大規模攻擊**，而無需具備高深專業知識，將導致網路犯罪更加普及。

- 案例：**2024** 年某銀行遭遇針對高階管理層的 **AI** 驅動釣魚攻擊，導致大量**機密資料外洩**。
- 企業應對策略：企業應採用 **AI** 驅動的偵測系統，如行為分析技術，及時發現異常行為。

網路釣魚

- 使用 AI 建立個性化釣魚電郵，如分析 LinkedIn 資料來針對受害者設計訊息

自適應惡意軟體

- 操縱訊息、塑造虛假的公眾輿論

量子計算將對加密技術構成新威脅

資安威脅九大面向

- 生成式AI多樣化
- **量子計算威脅**
- CIO 和 CISO 角色融合
- 勒索軟體影響供應鏈
- AI 驅動 SOC 助手
- 雲端安全平台主導
- AI 使用風險
- 深度偽造詐騙
- 物聯網攻擊面擴展

量子計算即將**挑戰現有的加密方法**。儘管大規模量子攻擊威脅形成尚需數年時間，但金融和醫療等產業必須及早開始採用**量子安全加密技術**，以有效抵禦這一近在眉睫的威脅。

現有的 **RSA 和 AES** 加密系統在量子計算前可能不堪一擊，與傳統計算相比，量子計算速度提高數百倍。

- 案例：一些國家已經開始採用量子加密技術來保護關鍵數據，如中國在軍事通訊中引入量子加密。
- 企業應對策略：投資研究**量子抗性加密技術（例如 lattice-based cryptography）**。

隨 AI 普及，資訊長和資安長角色趨於融合

資安威脅九大面向

- 生成式AI多樣化
- 量子計算威脅
- **CIO 和 CISO 角色融合**
- 勒索軟體影響供應鏈
- AI 驅動 SOC 助手
- 雲端安全平台主導
- AI 使用風險
- 深度偽造詐騙
- 物聯網攻擊面擴展

隨著企業日益採用 AI 和**導入混合雲環境，資訊長和資安長的角色將逐步整合** (傳統上 IT 和資安是分離的)，轉向全面風險管理。根據 Check Point 報告預測，資訊長將監管愈來愈多網路安全維運，推動 IT 與安全職能團隊之間更緊密的協作，能減少資源浪費：統一的策略能減少資源重複投入。

- 案例：一些公司將 **CIO 和 CISO 職位合併**，使資安策略更具協同性。
- 企業應對策略：**鼓勵 IT 和資安部門合作**，確保資安成為業務策略的一部分。

CISO

➢ Chief Information Security Officer

CIO

➢ Chief Information Officer

勒索軟體將重創供應鏈

資安威脅九大面向

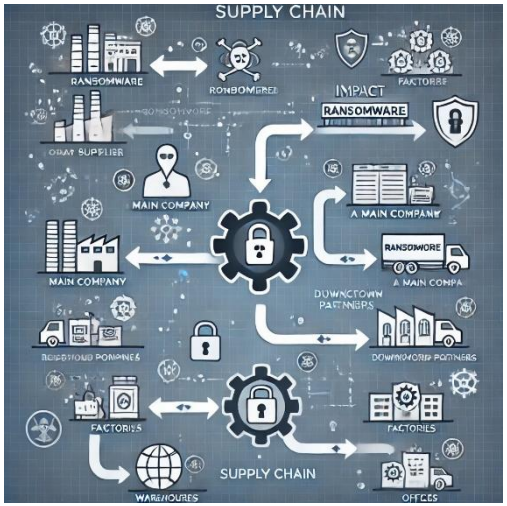
- 生成式AI多樣化
- 量子計算威脅
- CIO 和 CISO 角色融合
- **勒索軟體影響供應鏈**
- AI 驅動 SOC 助手
- 雲端安全平台主導
- AI 使用風險
- 深度偽造詐騙
- 物聯網攻擊面擴展

勒索軟體將變得更具**針對性**和**自動化**，並將攻擊矛頭指向**關鍵供應鏈**，大規模攻擊可能更加頻繁，影響整個產業。同時，攻擊者會**運用 AI 增強型網路釣魚電子郵件和深度偽造技術冒充身份**，以避開防禦系統。或者是攻擊者通過入侵供應鏈上的小型供應商，再間接威脅大型企業，進而強迫支付贖金。

與傳統攻擊比較，供應鏈攻擊擴大了影響範圍，增加受害者數量。

- 案例：
2023 年的 Kaseya 事件，攻擊者利用 IT 供應商的漏洞影響了上千家中小型企業，導致多家企業支付高額贖金。

- 企業應對策略：
增強**供應鏈風險管理**，確保供應商遵守資安標準，並定期審查供應鏈資安狀況。



AI 驅動的 SOC 助手將革新安全維運

資安威脅九大面向

- 生成式AI多樣化
- 量子計算威脅
- CIO 和 CISO 角色融合
- 勒索軟體影響供應鏈
- **AI 驅動 SOC 助手**
- 雲端安全平台主導
- AI 使用風險
- 深度偽造詐騙
- 物聯網攻擊面擴展

資訊安全監控中心（SOC）將利用 AI 助手處理大量資料並對威脅進行**優先順序劃分**，進而縮短回應時間。這些 AI 驅動的工具將有助於自動偵測威脅並減少誤報，藉此提升安全團隊效率。

1 提升威脅檢測速度與準確性

- 快速分析大量數據，縮短檢測時間
- 機器學習算法提高準確度
- 及時發現異常行為

2 自動化威脅優先排序

- 自動排序威脅的嚴重程度
- 集中資源處理高風險事件
- 確保即時應對關鍵威脅

3 減少誤報率，優化資源分配

- 過濾無關警報，減少誤報
- 讓團隊專注於真實威脅
- 提升資源使用效率

4 支持持續學習，適應新興威脅

- 持續學習新攻擊模式
- 自動更新應對流程
- 增強企業彈性與適應力

雲端安全平台主導市場

資安威脅九大面向

- 生成式AI多樣化
- 量子計算威脅
- CIO 和 CISO 角色融合
- 勒索軟體影響供應鏈
- AI 驅動 SOC 助手
- **雲端安全平台主導**
- AI 使用風險
- 深度偽造詐騙
- 物聯網攻擊面擴展

組織將遷移至整合式雲端安全平台，採用**雲端原生安全平台（CNAPP）**等工具來監控並保護多雲環境。**AI** 將在自動化威脅防禦上發揮關鍵作用，將重心從被動防護轉向主動防禦。

趨勢特徵

1. **集中管理多雲環境**：企業需要一個統一的安全平台，來簡化不同雲服務供應商間的安全操作，例如 **AWS**、**Azure** 和 **Google Cloud**，確保所有雲環境的安全性一致。

2. **增強可見性和控制力**：多雲環境的複雜性讓企業難以全面掌控其數據和應用的安全狀態，而統一的雲端安全平台能提供跨平台的可見性，便於即時監控和管理。

3. **符合合規性要求**：統一的安全平台可協助企業自動化合規流程，確保各雲環境中的數據存儲、傳輸和處理均符合相關的法規和安全標準。

企業面臨的挑戰

AI 使用不當將增加資料外洩風險

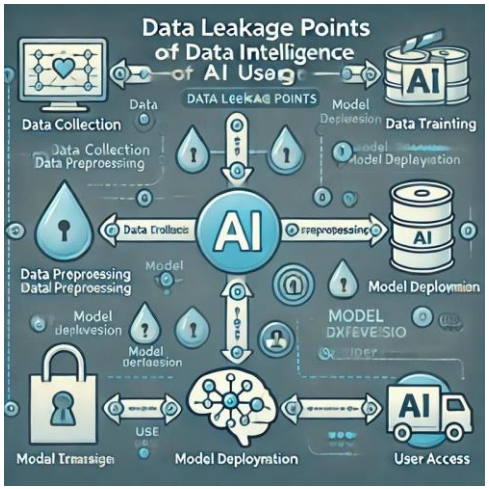
資安威脅九大面向

- 生成式AI多樣化
- 量子計算威脅
- CIO 和 CISO 角色融合
- 勒索軟體影響供應鏈
- AI 驅動 SOC 助手
- 雲端安全平台主導
- **AI 使用風險**
- 深度偽造詐騙
- 物聯網攻擊面擴展

隨著 ChatGPT 等 AI 工具成為業務流程中不可或缺的一部分，意外的資料外洩將成為重要隱憂。員工可能在無意間將敏感資料分享給外部 AI 平台，導致非蓄意的資料外洩。組織需要建立治理架構來監控 AI 使用情況並保護資料隱私。

趨勢特徵

1. **數據洩露風險**：AI 模型在訓練和預測過程中可能意外暴露敏感數據，增加資料外洩風險。
2. **偏見和不公平性**：如果模型訓練數據不平衡，AI 系統可能會對特定群體產生偏見，進而影響業務決策。
3. **合規挑戰**：AI 系統可能涉及大量個人數據，增加企業遵守隱私法規（如 GDPR、CCPA）的挑戰。



社群媒體濫用和深度偽造技術將屢見不鮮

資安威脅九大面向

- 生成式AI多樣化
- 量子計算威脅
- CIO 和 CISO 角色融合
- 勒索軟體影響供應鏈
- AI 驅動 SOC 助手
- 雲端安全平台主導
- AI 使用風險
- **深度偽造詐騙**
- 物聯網攻擊面擴展

愈來愈多的網路犯罪分子將瞄準社群媒體平台，利用**個人資訊實施精準詐騙和身份冒充**。AI 驅動的深度偽造技術將更加逼真，對**金融交易**和**企業安全**構成威脅。為了偵測並防範這些複雜攻擊，企業需要採用即時 AI 防禦。

深度偽造（Deepfake）技術利用 AI 生成人臉、語音和影像，能高度逼真地模仿真實人物。該技術在**影像合成、聲音模擬**等方面發展迅速，使詐騙活動有了新的突破口。深度偽造詐騙通常用於**身份冒充、金融詐騙**等，企業、政府及個人均可能成為目標。

企業應對策略:

1. **引入 AI深度偽造檢測技術**，幫助識別視覺或聽覺上的偽造內容。
2. **建立多層次身份驗證機制**：採用**多因子認證（MFA）和生物識別技術**，加強身份核實流程。

物聯網擴展增大攻擊面

資安威脅九大面向

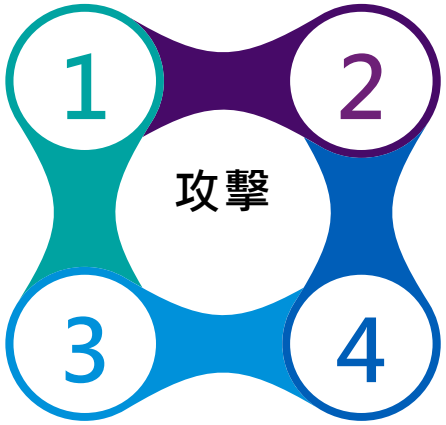
- 生成式AI多樣化
- 量子計算威脅
- CIO 和 CISO 角色融合
- 勒索軟體影響供應鏈
- AI 驅動 SOC 助手
- 雲端安全平台主導
- AI 使用風險
- 深度偽造詐騙
- 物聯網攻擊面擴展

預計到了 2025 年物**聯網裝置數量將達到 320 億台**，確保這些互連系統的安全將變得至關重要，攻擊者將利用安全防護脆弱的物聯網裝置入侵雲端網路。為了降低此風險，組織必須採用零信任架構和 AI 威脅偵測工具。

對**5G基礎設施**的一次成功攻擊，可能輕而易舉地就破壞了關鍵產業，如**石油、天然氣、交通、公共安全、金融**和**醫療**等。

5G攻擊

網路活動被外推至分散式數位路由器，消除了阻塞點檢查和控制的可能性。



代理網路戰

將資安攻擊外包至非法駭客組織，並藉由網域名稱系統系統隧道、或憑證填充等形式進行攻擊

零日漏洞(零時差)

- 帳號接管(ATO) 攻擊
- 水抗攻擊
- 零日星期三

資訊戰

- 操縱訊息、塑造虛假的公眾輿論

機關如何面對未來趨勢？

- ✓ 建立全面的資安架構，如**零信任架構(Zero Trust Architecture)**，確保所有內外部訪問均須經過驗證與授權。
- ✓ 加強**供應鏈**和**雲端安全防護**，降低工作流程風險性。
- ✓ 應對AI驅動的威脅，如使用**AI偵測工具**識別異常行為和深度偽造內容。
- ✓ 投資新技術和**量子計算防護**，實驗並佈署基於AI的SOC工具，提升威脅檢測效率。
- ✓ 具備**洞察威脅趨勢的敏感度**，並擴大IT人員的管控範圍與責任。
- ✓ 具備全天候的**安全威脅檢測**，確保雲端、電子郵件、端點及網路服務安全性，並確認安全警報的優先順序。

個人如何面對未來趨勢？

- ✓ 提升**數位安全意識與能力**，定期學習最新的資安威脅(如AI驅動詐騙、深度偽造)和防護方法。
- ✓ 強化**個人數據的保護**，啟用多因子身分驗證(MFA)或採用密碼管理工具生成和保存密碼。
- ✓ 識別並防範深度偽造和AI驅動的威脅，須提升自我**資訊判讀意識**。
- ✓ 使用**防毒軟體**，為裝置加強防護，主動偵測惡意網頁與郵件。
- ✓ 慎防**網路釣魚**，不隨意點擊不明連結或下載檔案，小心與疫情相關的惡意威脅。

KPMG

Thank you