115學年度聖母醫護管理專科學校

校園資訊安全通識教育訓練

📋 課程資訊

- **日期時間：** 115 年 10 月 30 日（五）13:10 – 16:10
- **研習地點：** G202教室
- **講座講師：** 國立宜蘭大學　游育豪 講師
- **主辦單位：** 聖母醫護管理專科學校 宜蘭區域網路中心
- **課程主軸：** Part 1 資訊安全基本概念 ｜ Part 2 資安事件分享

校園資訊安全通識教育訓練

提升資安意識・守護數位校園

PART 1　資訊安全基本概念

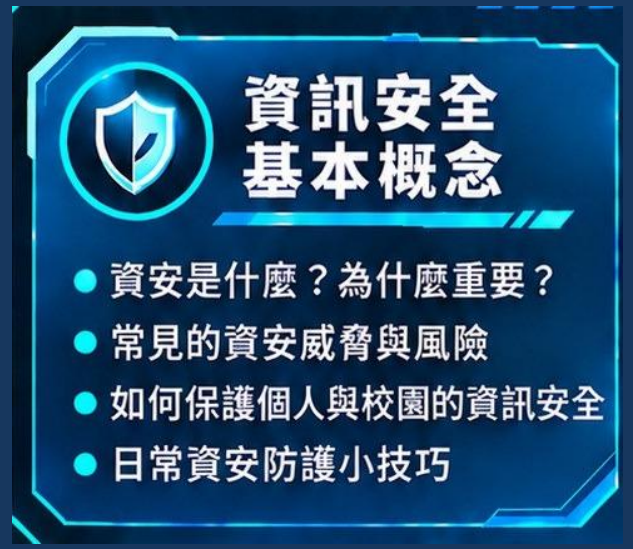
PART 2　資安事件分享



115年10月30日（五）
13:10–16:10 | G202 教室

國立宜蘭大學　講師：游育豪

Agenda

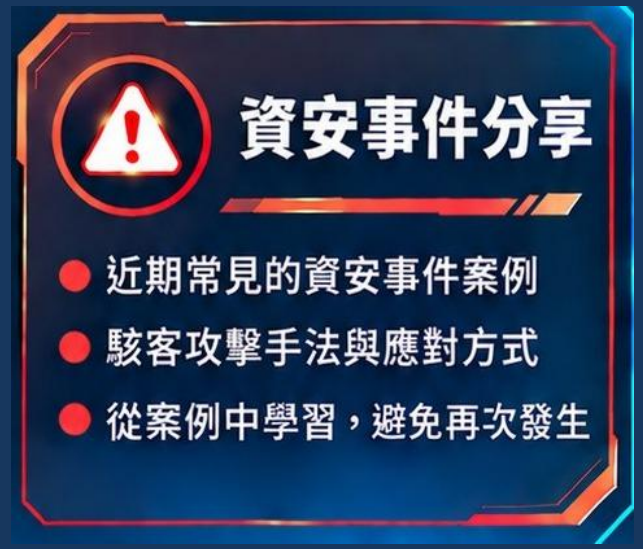


01 資安是什麼？為什麼重要？

02 常見的資安威脅與風險

03 如何保護個人與校園的資訊安全

04 日常資安防護小技巧



05 近期常見的資安事件案例

06 駭客攻擊手法與應對方式

07 從案例中學習，避免再次發生

08 課後測驗與綜合討論

PART 1

資訊安全基本概念

01 資安是什麼？為什麼重要？

02 常見的資安威脅與風險

03 如何保護個人與校園的資訊安全

04 日常資安防護小技巧





資安是什麼？資訊安全的三大核心 C · I · A

C 機密性
Confidentiality

只有被授權的人才能看

例：學生成績、家長聯絡資料、實習病患資料不外流

I 完整性
Integrity

資料正確、不被竄改

例：成績、公文金額、網站公告不被偷偷修改

A 可用性
Availability

需要時系統能正常使用

例：選課、校務系統、電子郵件不中斷（勒索軟體專攻這點）

資安 = 保護「資料」與「系統」：讓對的人、在對的時間、拿到正確的資料



為什麼重要？校園為什麼是駭客眼中的目標

1 個資寶庫

學生、家長、教職員個資，護理實習還會接觸病患資料

2 人多帳號多

師生人數多、流動快，一個弱密碼就是破口

3 環境開放

校園網路開放，電腦、手機、實驗設備、IoT 種類多

4 資源有限

資安人力與預算有限，駭客專挑防護較弱的對象

一旦出事，代價是...

- 教學與行政停擺，系統被鎖、無法上課選課
- 個資外洩，學校與個人負個資法責任
- 學校商譽與家長信任受損
- 復原費時費力，甚至遭二次勒索

資安威脅持續惡化

- 台灣2024年遭受攻擊次數較2023年翻倍成長，2025年持續攀升，平均每天高達數萬次攻擊
- 2026年網路安全預測：全球資安戰場正式邁入「AI攻擊全面實戰化」時代
- 案例：跨國企業遭AI深偽（deepfake）視訊詐騙，仿冒財務長要求員工匯款，損失約2億港元（約新台幣8億元）

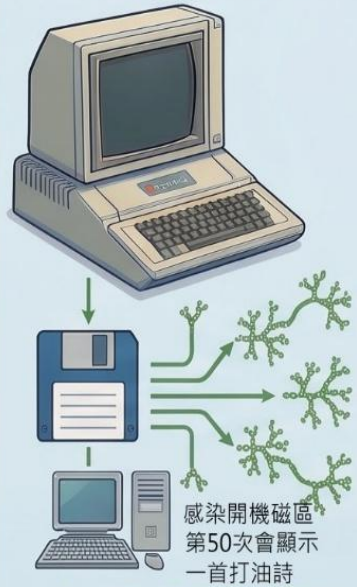
YouTube



資安攻擊每十年也跟著變化

1980 | 1990 | 2000 | 2010 | 2020 | 2030

病毒萌 芽期



病毒萌芽期

1982年-Elk Cloner首
首個廣泛傳播的個人
電腦病毒透過Apple II
軟碟傳播

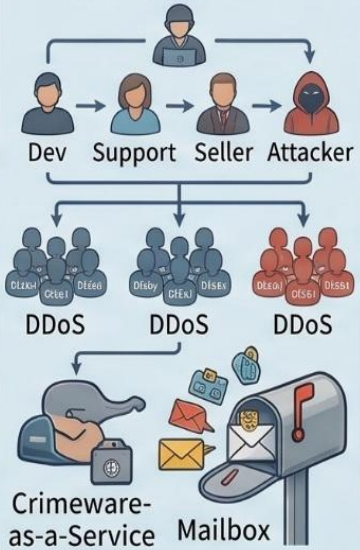
CIH病毒功能



網路化攻擊

CIH病毒1998-台灣
製作，可破壞BIOS
造成破體實質損毀
全球災情修重
駭客組織成形

網絡犯罪產業



網路犯罪產業化

2000年起~
蠕蟲全球大爆發
殭屍網路DDOS網路
犯罪商業化釣魚郵件
出現

國家級網軍T攻擊



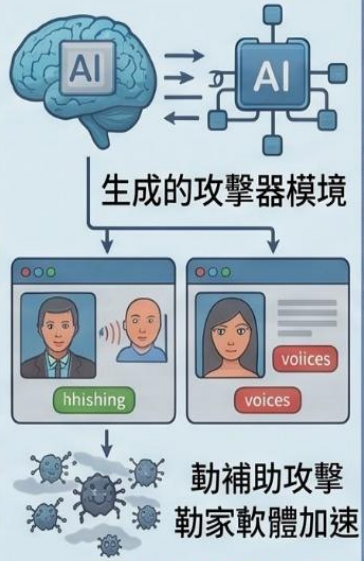
國家級-網網軍
大規模資料外澄常態化



國家級網軍
資料外洩常態化

2010年起~
國家級網軍
APT攻擊
大規模資料外瀆常態化
勒索軟體出現
CryptoLocker
WannaCry

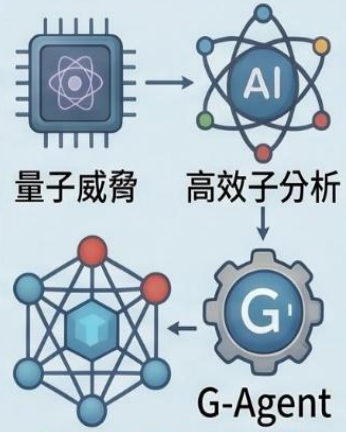
AI電腦攻擊



AI電腦攻擊與
全自動化

生成式AI武發化
Deepfake詐騙
AI補助攻擊
Agentic AI攻擊
勒索軟體加速
2020年起~

未來的資安威脅



未來的資安
威脅

2030年起~
量子威脅
全自動攻防
深偽即時化
AI Agent治理風險
2030年+起~

優業網絡



六大常見威脅：多數攻擊都從「人」開始

1 社交工程 / 釣魚

假冒郵件、簡訊、電話，騙你點連結、輸入帳密

2 惡意程式 / 勒索軟體

檔案被加密勒索、資料被偷，系統全面停擺

3 帳號密碼外洩

弱密碼、一組密碼走天下，遭「撞庫」盜用

4 個資外洩

誤寄、雲端分享權限錯誤、貼進免費 AI 工具

5 詐騙與深偽

AI 換臉換聲，假冒長官或親友要求匯款

6 設備與網路風險

系統未更新、來路不明 USB、公共 Wi-Fi、IoT

AI可以被訓練成有道德 沒有道德



2026五大資安威脅趨勢

深偽 AI 攻擊

換臉、換聲視訊詐騙企業高層

勒索軟體與資料竊取

持續進化、自動化程度提高

影子代理（Shadow Agent）風險

每人平均擁有約8個數位代理人/助理，一旦身份遭冒用即等同「被取代」

國家級攻擊

具政治與經濟目的之高階威脅

供應鏈攻擊

透過第三方廠商或維修人員迂迴入侵

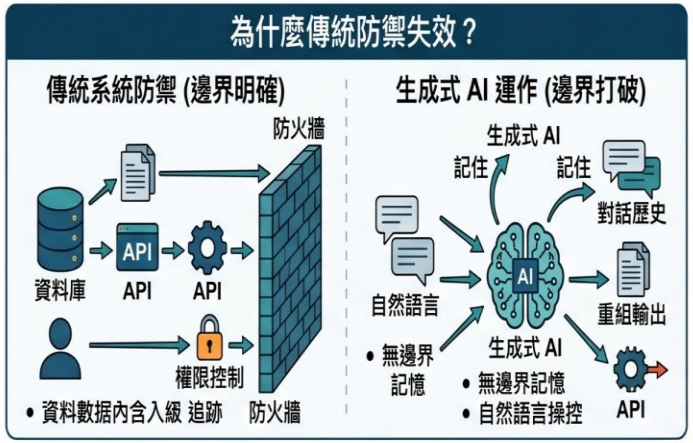
攻擊速度大幅壓縮（AI加持後）

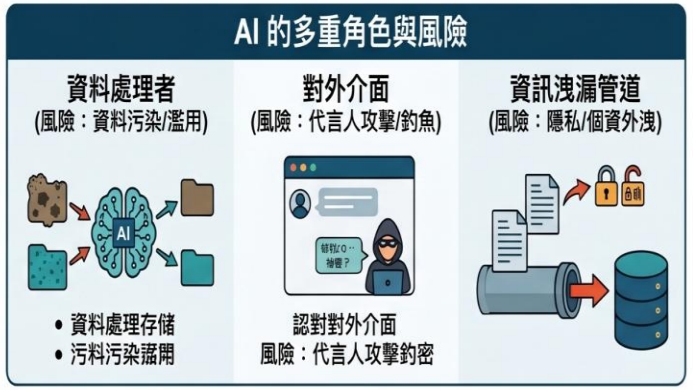
- 建構勒索軟體：12小時 → 3小時 → 2026年僅需15分鐘
- 入侵滲透：9天 → 1天 → 2026年僅需20分鐘

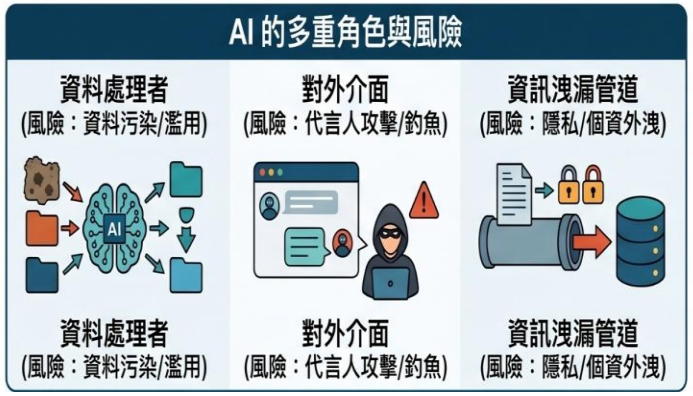


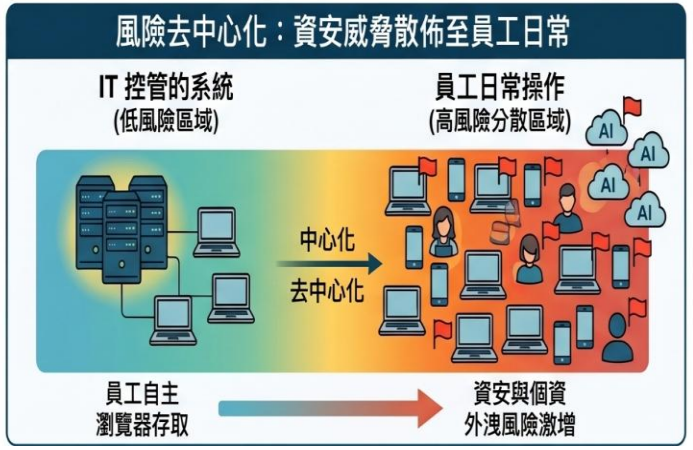
使用 AI 時，資安與個資最容易被忽略

- 傳統系統的資安邊界相對清楚：資料庫、API、權限。但生成式 AI 打破了這個邊界——它會「記住」對話、會被自然語言操控、會把多份內部文件的內容重新組合輸出。
- AI 同時是一個資料處理者、一個對外介面，也是一個可能洩漏資訊的管道。
- AI 工具導入門檻極低，同仁只要打開瀏覽器就能使用。這代表資安風險不再只發生在 IT 控管的系統內，而是分散在每一位同仁的日常操作中。若沒有加以管理限制，資安與個資外洩風險就很大。



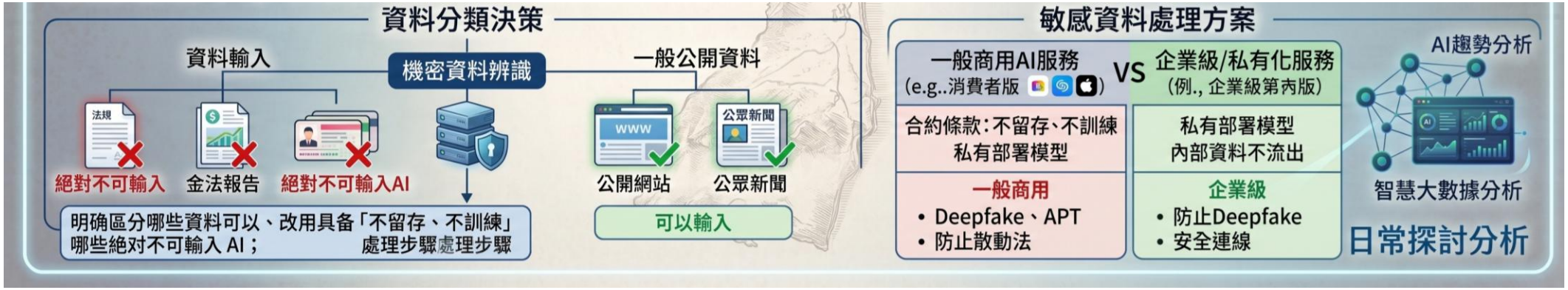






使用 AI 的風險：訓練與對話資料外洩

- 最常見的事故，是同仁為了讓 AI 回答得更準確，直接把學生名冊、合約、成績或財務報表貼進公開的 AI 服務。這些內容可能被服務商用於後續訓練，或在記錄中被保留，等同把機密資料交給了第三方。
- 防護重點：明確區分哪些資料可以、哪些絕對不可輸入 AI；對需要處理敏感資料的場景，改用具備「不留存、不訓練」合約條款的學校核准的企業版或校內自建模型。



影子 AI（Shadow AI）與未授權工具使用

- 當學校沒有提供合規的 AI 工具，同仁往往會自行使用各種免費服務來提升效率，形成 IT 無法掌握的「影子 AI」。這些工具的資料政策、安全等級參差不齊，是資料外洩的高風險來源。
- 防護重點：與其全面禁止，不如提供一套安全、好用的官方 AI 工具，並搭配清楚的使用政策與教育訓練，把同仁的使用行為導回可控管的環境。





高風險資料→絕對不能告訴 AI 的資訊

個人身分

例：身分證號、護照號
風險：可能被用於身份盜竊

金融資訊

例：信用卡號、銀行帳密
風險：直接的財務風險

公務機密

例：未公開公文、招生與預算規劃
風險：損害學校權益與信任

學生 / 病患資料

例：學生名冊、成績、實習病患資料
風險：違反個資法

密碼憑證

例：任何帳號密碼
風險：安全漏洞

法律文件

例：合約細節、訴訟內容
風險：律師—客戶特權失效

各家 AI 的隱私政策（2026 最新）

面向	ChatGPT	Claude	Gemini	Perplexity
預設用對話訓練模型	⚠ 可關閉	✗ 不會	⚠ 可關閉	✗ 不會
如何關閉	設定 → Data Controls	預設即關	活動 → 關閉	預設即關
企業版隱私	✓ Enterprise	✓ Team/Enterprise	✓ Workspace	N/A
資料保存期	30 天	90 天	依設定	不保存
GDPR 合規	✓	✓	✓	✓

資料為政策重點摘要，實際規範以各平台最新官方隱私權政策為準



資安是團隊運動：每個人都是第一道防線

個人做得到

- 帳號密碼不共用、不外借，開啟多因子驗證
- 電腦、手機、防毒軟體保持更新
- 離開座位鎖定螢幕（Win + L）
- 不明連結、附件先查證再點
- 個資最小化：不該收的不收、不該傳的不傳

校園一起做

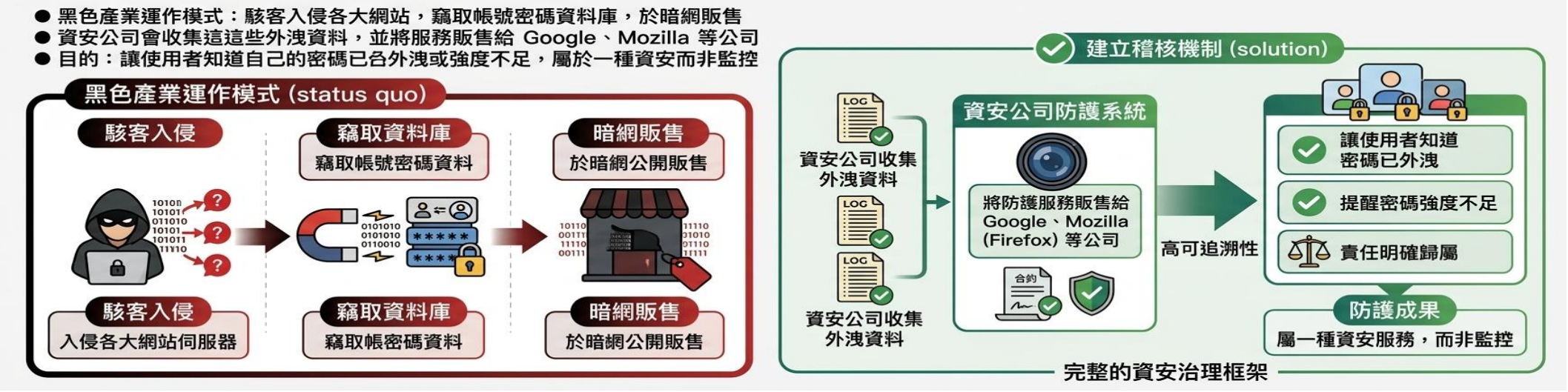
- 遵守學校資安政策與個資保護規範
- 使用學校核准的軟體與雲端服務（含 AI）
- 重要資料定期備份到學校指定位置
- 公務資料分級保護，分享前確認權限
- 發現異常立即通報資訊單位，不自行處理

最強的防火牆，是有資安意識的人

密碼與帳號安全

密碼外洩是怎麼被發現的？

- 黑色產業運作模式：駭客入侵各大網站，竊取帳號密碼資料庫，於暗網販售
- 資安公司會收集這些外洩資料，並將服務販售給 Google、Mozilla（Firefox）等公司
- 目的：讓使用者知道自己的密碼已外洩或強度不足，屬於一種資安服務，而非廠商本身監控你



密碼與帳號安全

常見密碼安全機制的迷思

(一) 密碼複雜度規則已經過時

- 可從密碼規則判斷網站是否安全：若網站限制密碼「不能超過8字」，代表系統老舊（如早期BBS）
- 過去要求「大小寫＋特殊符號」是因應CPU/顯卡暴力破解年代的產物
- 美國NIST最新建議：密碼長度（14-20字或一句話）遠比複雜度重要原因：字元集每多一種只是「線性增加」，長度每多一位是「指數增加」運算量

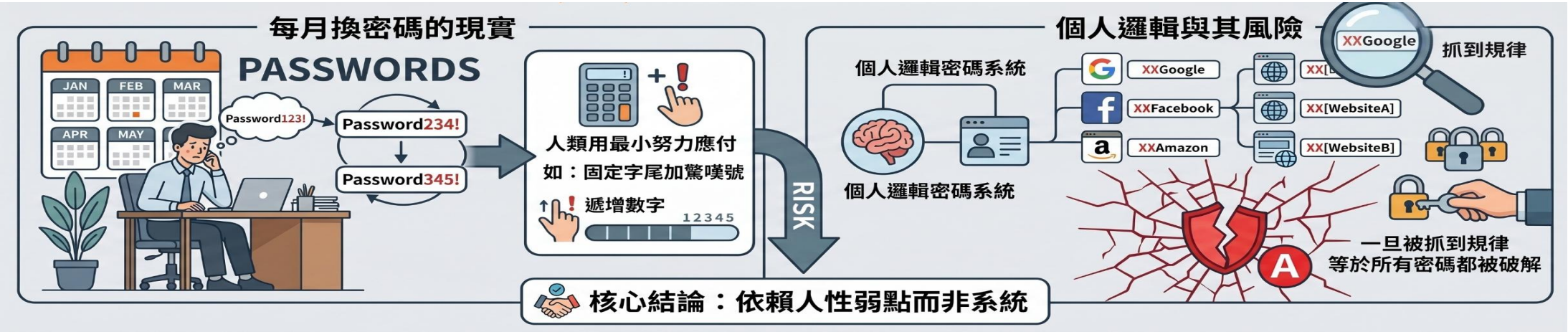




常見密碼安全機制的迷思

(二)人性使複雜度規則失效

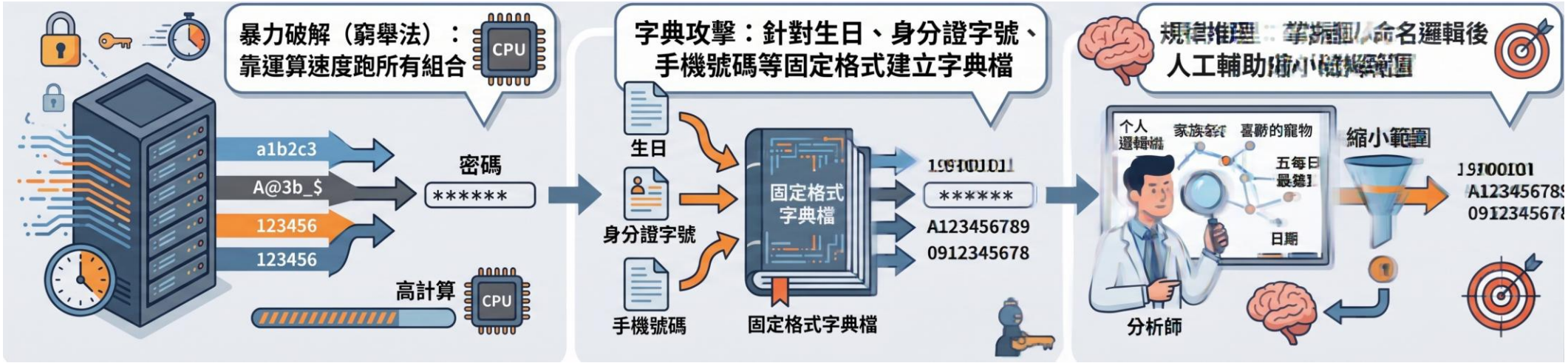
- 強制每月換密碼 → 人類會用最小努力應付規則（如：固定字尾加驚嘆號、遞增數字）
- 若密碼具有個人邏輯規律（如本名注音、幫不同網站加字尾如「XXGoogle」），一旦被抓到規律，等於所有密碼都被破解



常見密碼安全機制的迷思

(三)破解手法分類

- 暴力破解（窮舉法）：靠運算速度硬跑所有組合
- 字典攻擊：針對生日、身分證字號、手機號碼等固定格式建立字典檔
- 規律推理：掌握個人命名邏輯後，人工輔助縮小破解範圍



密碼管理工具

- 使用密碼管理工具管理兩三百組密碼，每次登入都換成隨機高強度密碼
- 核心優勢：只需要記住「一組主密碼」保護工具本身
- 附加防護：能自動核對網址是否與存檔一致，可用來識別釣魚網站（如將字母 l 換成 1 的偽冒網域）
- 重要提醒：若密碼已大量外洩，一般民眾沒有「一鍵全部更換」的簡單方法，仍需一組一組改（企業級才有代管方案）





免費好用的密碼管理工具推薦

Enpass

雲端型

- 電腦、手機、瀏覽器都能用
- 提供免費版 25組

前往官網 ›

KeePassXC

本地型・開源

- 資料庫存在自己電腦，完全免費
- 需自行備份與同步
- 適合想完全掌控資料的人

前往官網 ›

Proton Pass

雲端型・重隱私

- 免費版不限密碼與裝置
- 可產生電子郵件別名
- 保護真實信箱不外洩

前往官網 ›

內建工具

免安裝・最易上手

- Chrome / Android：Google 密碼管理工具
- iPhone / Mac：「密碼」App
- 適合剛開始使用的人

Google ›　Apple ›

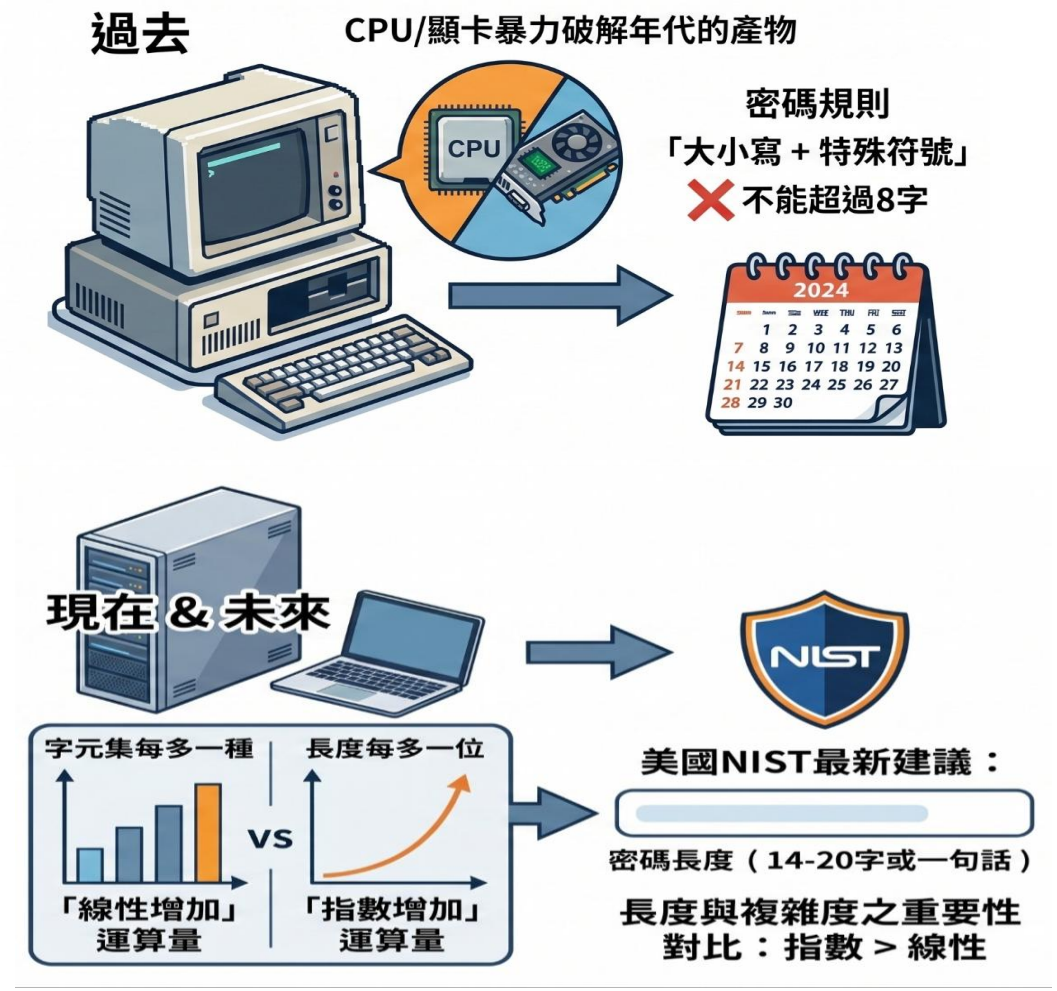
選擇原則：主密碼夠長且只用在這裡・務必開啟多因子驗證・只從官網或官方商店下載

功能與免費方案內容以各官網最新說明為準

密碼與帳號安全

更換密碼的建議策略

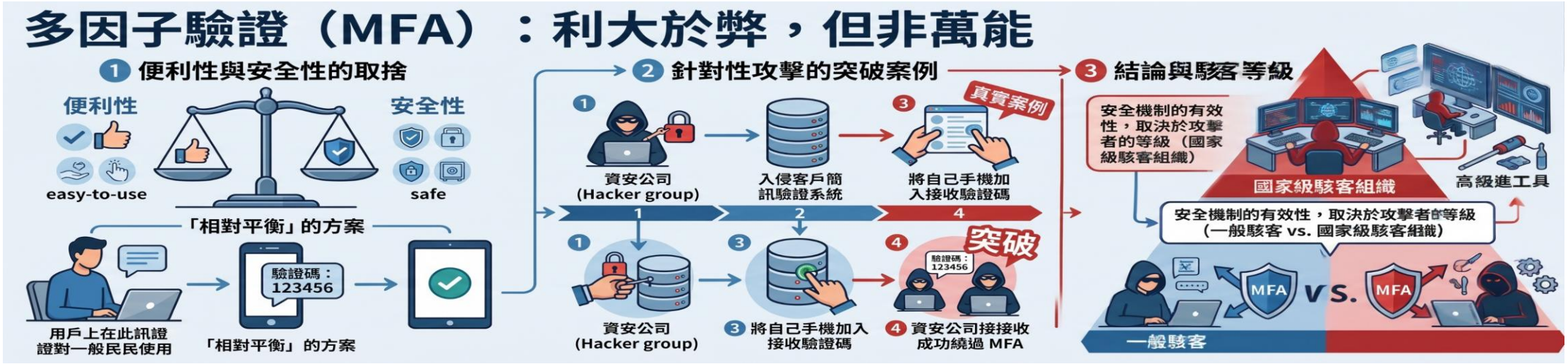
- 不建議依「固定週期」換密碼（NIST建議：密碼夠長、夠獨特就不必換，除非網站通知外洩）
- 一般人可採帳號分級策略：
- 最高風險（銀行、學校公務帳號）→ 獨一無二、高強度密碼
- 中風險（購物網站）→ 次要密碼
- 低風險（論壇、遊戲）→ 可共用較簡單密碼



密碼與帳號安全

多因子驗證（MFA）：利大於弊，但非萬能

- 簡訊二階段驗證（OTP）對一般民眾是「相對平衡」的方案（便利性與安全性的取捨）
- 案例證明：即使有OTP保護，若驗證碼發送系統本身存在漏洞，仍可被繞過（曾有資安公司入侵客戶簡訊系統、加入自己手機接收驗證碼）
- 結論：MFA/OTP 的實際防護力，取決於背後系統本身是否足夠安全，而非只看使用者有沒有開啟這個功能；同時，是否值得投入資源攻破，也與攻擊者鎖定的目標等級有關



密碼與帳號安全

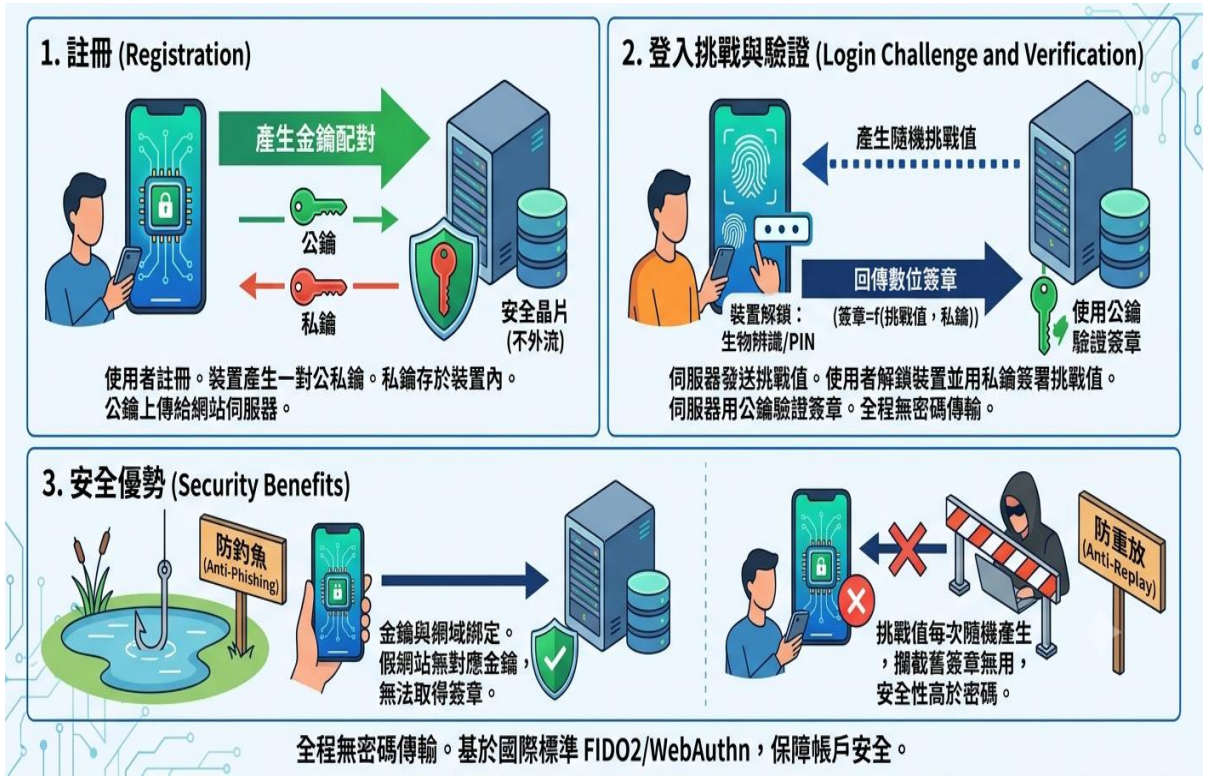
多因子驗證（MFA）：利大於弊，但非萬能

- Face ID / Touch ID → 降低輸入成本，改用生物特徵驗證
- Passkey：免密碼、難以被破解，未來密碼可能會完全消失（過渡期間仍需與傳統帳密並存）

1.公私鑰配對：註冊時裝置產生一組公私鑰，私鑰永久存於裝置安全區域（不外流），公鑰上傳給網站保管。

2.挑戰簽章驗證：登入時網站發出隨機挑戰值，裝置經生物辨識/PIN解鎖後用私鑰簽章回傳，網站以公鑰驗證簽章正確性，全程不傳輸密碼本身。

3.防釣魚與防重放：金鑰與網域綁定（假網站無法取得有效簽章），且挑戰值每次隨機產生，即使被攔截也無法重複使用，安全性遠高於傳統密碼。



設備安全

IoT設備風險：你的智慧燈泡也能是跳板

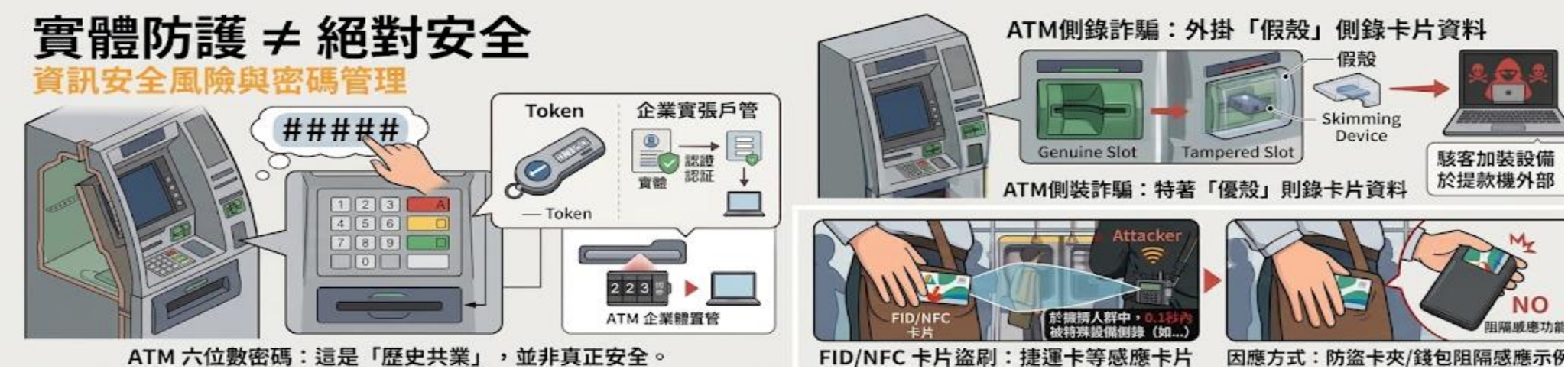
- 智慧電燈等聯網裝置若安全性設定不足，可能被駭客當作跳板攻擊（如攻擊政府單位）
- 一旦被用作跳板，執法單位追查IP時，屋主可能無辜背上攻擊嫌疑
- 核心觀念：任何聯網設備背後都有作業系統，被入侵即可被遠端操控



實體安全

實體防護 ≠ 絕對安全

- ATM 六位數密碼：這是「歷史共業」，並非真正安全的設計（企業戶則多搭配Token實體裝置）
- ATM側錄詐騙：駭客會在提款機外部加裝「假殼」側錄卡片資料
- FID/NFC 卡片盜刷：捷運卡等感應式卡片可能在擁擠人群中，於一秒內被特殊設備側錄因應方式：市面已有專門阻隔感應的防盜卡夾/錢包





日常資安防護 10 招：今天就能開始做

1	**長密碼 / 密碼句**	14 字以上、各網站不同，交給密碼管理工具	6	**3-2-1 備份**	3 份資料、2 種媒體、1 份離線或異地
2	**開啟多因子驗證**	學校信箱、銀行、社群帳號優先開啟	7	**慎用公共 Wi-Fi**	不在公共網路登入重要帳號，可改用行動網路
3	**自動更新**	作業系統、瀏覽器、App 一有更新就安裝	8	**USB 不亂插**	來路不明的隨身碟不要插公務電腦
4	**先查證再點**	急迫、要錢、要帳密的訊息，一律先停	9	**個資不外流**	不貼進免費 AI，雲端分享設定「指定對象」
5	**鎖定螢幕**	離開座位按 Win + L，手機設定螢幕鎖	10	**異常就通報**	中毒、被盜、誤寄，第一時間通報資訊單位

日常資安防護小技巧

護理專科專屬｜把「護理專業好習慣」化為最強資安防線

💉 連線與核對：資安「三讀五對」

給藥要三讀五對；收信、點網址、傳檔案也要三讀五對！

- **三讀：** 收信看真正寄件人、點擊懸停核對網址、送出前檢查有無夾帶個資。
- **五對：** 對象對、網址對、附件對、授權對、病歷與個案去識別化對。

💊 護理站感控：離座順手「Win + L」

推車不上鎖，針劑會短少；離座不鎖機，個資隨人跑！

- **感控比喻：** 如同接觸病人要洗手；離座的「數位洗手」就是 Win+L 鎖定！
- **多人共用：** 護理站、研究室公用電腦離開必鎖定，防止病歷與成績遭竄改窺探。

🤖 實習報告問 AI：謹記「三不去」

實習報告問 AI，病歷個資絕不帶；床號姓名去識別，特種個資不上雲！

- **法規紅線：** 依個資法第 6 條，病歷、醫療、健檢屬特種個資，外洩負刑責與重罰！
- **三不去原則：** 去姓名身分、去床號與特殊時間、去病灶與傷口醫療照片。

🚨 中毒異常應變：如臨感控「先拔線做隔離」

電腦染疫第一步，立刻拔線做隔離；通報如同喊急救，聯絡網中莫遲疑！

- **阻斷傳播：** 發現傳染病先隔離；電腦遇勒索軟體，第一時間拔網路線、關 Wi-Fi！
- **迅速通報：** 切斷區網橫向感染路徑，並即刻通報學校資訊組與宜蘭區網中心。

PART 2

資安事件分享

05 近期常見的資安事件案例

06 駭客攻擊手法與應對方式

07 從案例中學習，避免再次發生



近期常見的資安事件案例

從新聞看見風險：這些事件離我們並不遠

2024.01 | 深偽視訊詐騙

跨國企業員工被 AI 假冒的財務長與同事騙走約 2 億港元

相關報導 ›

2024.03 | 7 校校務系統遭駭

逾 2 萬筆學生個資在國外駭客網站兜售

相關報導 ›

2025.02 | 馬偕醫院勒索軟體

數百台電腦當機，北淡兩院區急診受影響

相關報導 ›

2025.03 | 彰基遭同組織攻擊

衛福部定調為「系統性攻擊」

相關報導 ›

2025.11 | 國安局抽驗 AI

5 款 AI 被驗出隱私蒐集、資料回傳等疑慮

相關報導 ›

2026.08 | AI 代理人越界

英國 AISI 測試記錄 19 次 AI 代理人未授權行動

相關報導 ›

資料來源：衛福部、教育部、國安局公告及 iThome、聯合報等公開報導整理（點「相關報導」開啟原文）

近期常見的資安事件案例

案例一｜醫療院所遭勒索軟體攻擊（2025）

發生什麼事

- 2025 年 2 月馬偕醫院遭 CrazyHunter 勒索軟體攻擊，數百台電腦當機、急診受影響
- 3 月彰化基督教醫院也遭同一組織攻擊
- 衛福部定調「系統性攻擊」，成立應變小組進駐
- 調查局後續查出有個資遭售予不法集團

駭客怎麼做

- 取得多名醫師的電子郵件帳號密碼
- 以外洩帳密登入，突破防護進入主機
- 加密資料庫與電腦，讓系統癱瘓
- 竊取資料並揚言兜售施壓（雙重勒索）

我們學到什麼

- 一組外洩的帳密，就能讓整個機構停擺
- 公務帳號開啟多因子驗證，密碼不重複使用
- 重要系統做離線備份，並演練復原
- 實習場域同樣是目標，病患資料格外保護

延伸閱讀

- iThome｜馬偕事件
- 衛福部說明
- iThome｜CrazyHunter 專題



案例二｜7 所高中校務系統遭駭、學生個資外洩（2024.03）

發生什麼事

- 7 所使用同一廠商校務行政系統的高中遭入侵
- 逾 2 萬筆學生個資在國外駭客網站兜售
- 駭客回頭向系統廠商勒索
- 教育部公布受影響學校，清查學習歷程等資料

駭客怎麼做

- 利用其中一校系統的漏洞入侵主機
- 竊得帳號密碼後，登入其他學校的系統
- 同一套系統、同一組弱點，一次波及多校（供應鏈風險）

我們學到什麼

- 委外系統也要定期弱點掃描與修補
- 不同系統不共用帳密，管理帳號開 MFA
- 合約明訂廠商資安責任與通報時限
- 學生個資最小化蒐集與保存

延伸閱讀

聯合報｜公布名單

聯合報｜個資外洩

今周刊｜校園資安人力

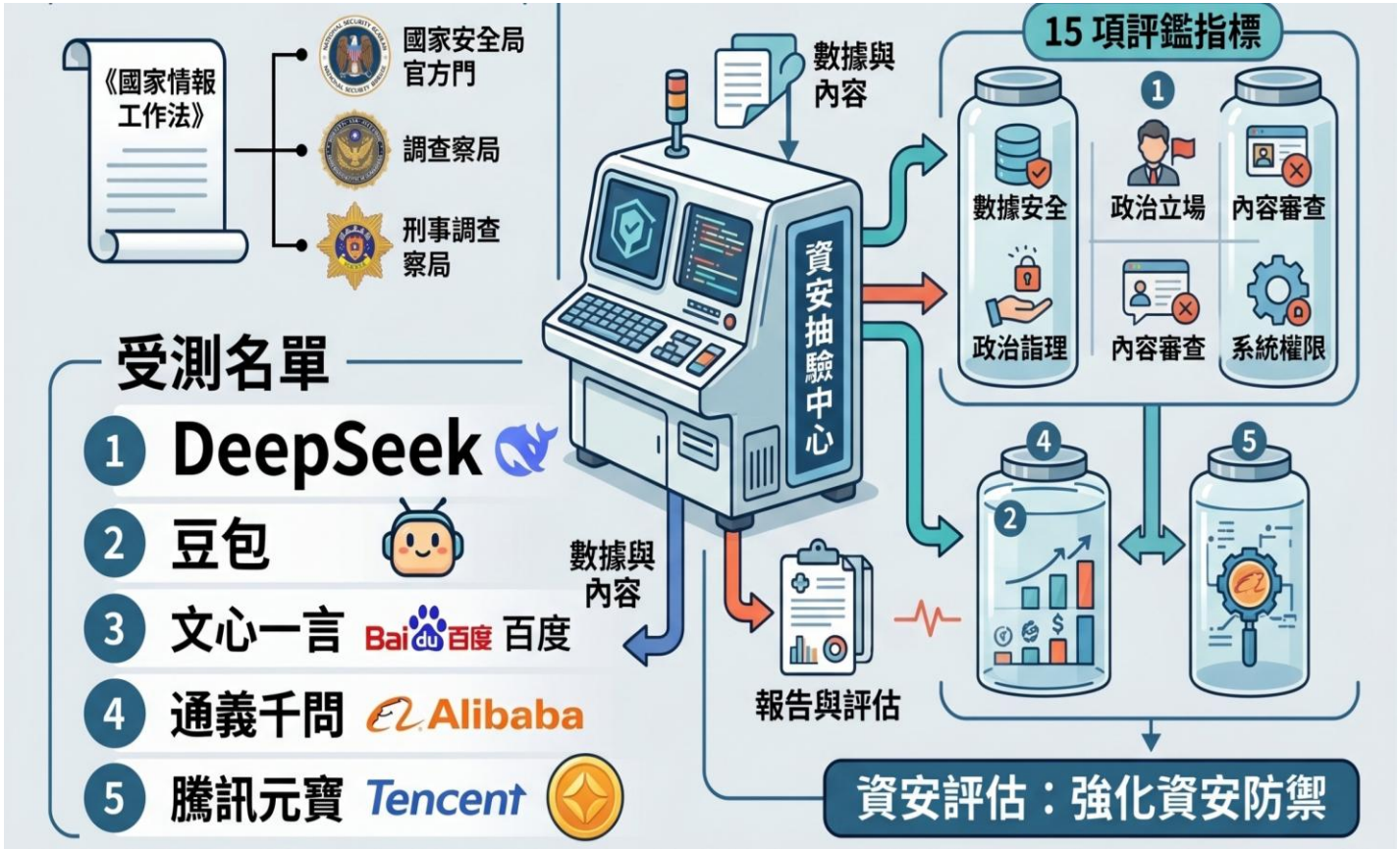
5款生成式AI模型存在資安風險

五款有資安疑慮生成式AI語言模型

相關報導：聯合報 | iThome | 公視新聞

- 國家安全局依《國家情報工作法》，會同調查局、刑事警察局，針對五款具代表性的中國大陸開發生成式 AI 語言模型進行資安抽驗，採用 15 項評鑑指標（涵蓋數據安全、政治立場、內容審查、系統權限等面向）。

- **受測 5 款生成式 AI 名單：**
- 1. DeepSeek：深度求索（開源推論模型）
- 2. 豆包 Doubao：字節跳動（TikTok 母公司）
- 3. 文心一言 ERNIE：百度 Baidu
- 4. 通義千問 Qwen：阿里巴巴 Alibaba
- 5. 騰訊元寶 Hunyuan：騰訊 Tencent



5款AI服務四大資安問題

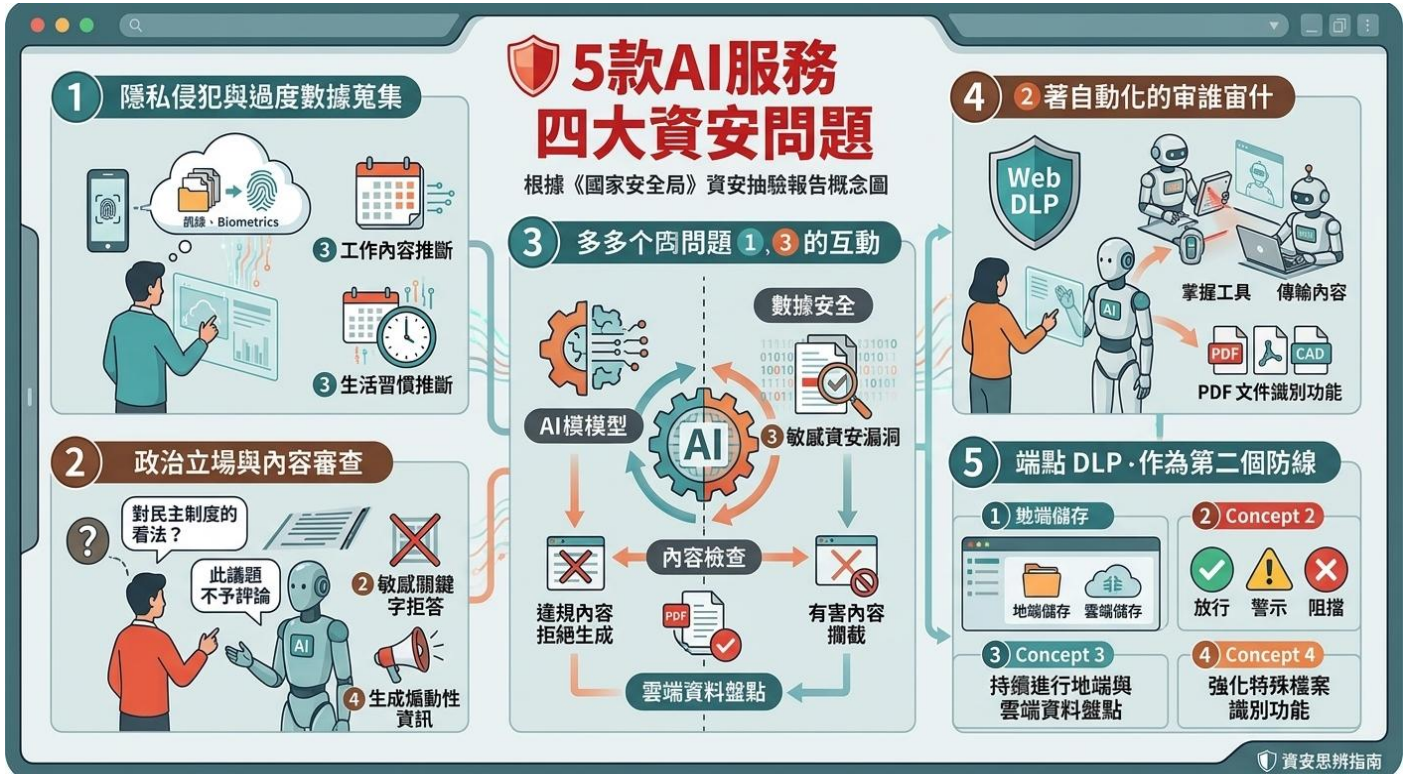
- **1. 隱私侵犯與過度數據蒐集**

越權存取使用者個資、掌握生物特徵
即使未開啟 App，仍可能在背景讀取手機內文件、圖片

可透過使用行為數據流量，推斷使用者工作內容與生活習慣

- **2. 政治立場與內容審查**

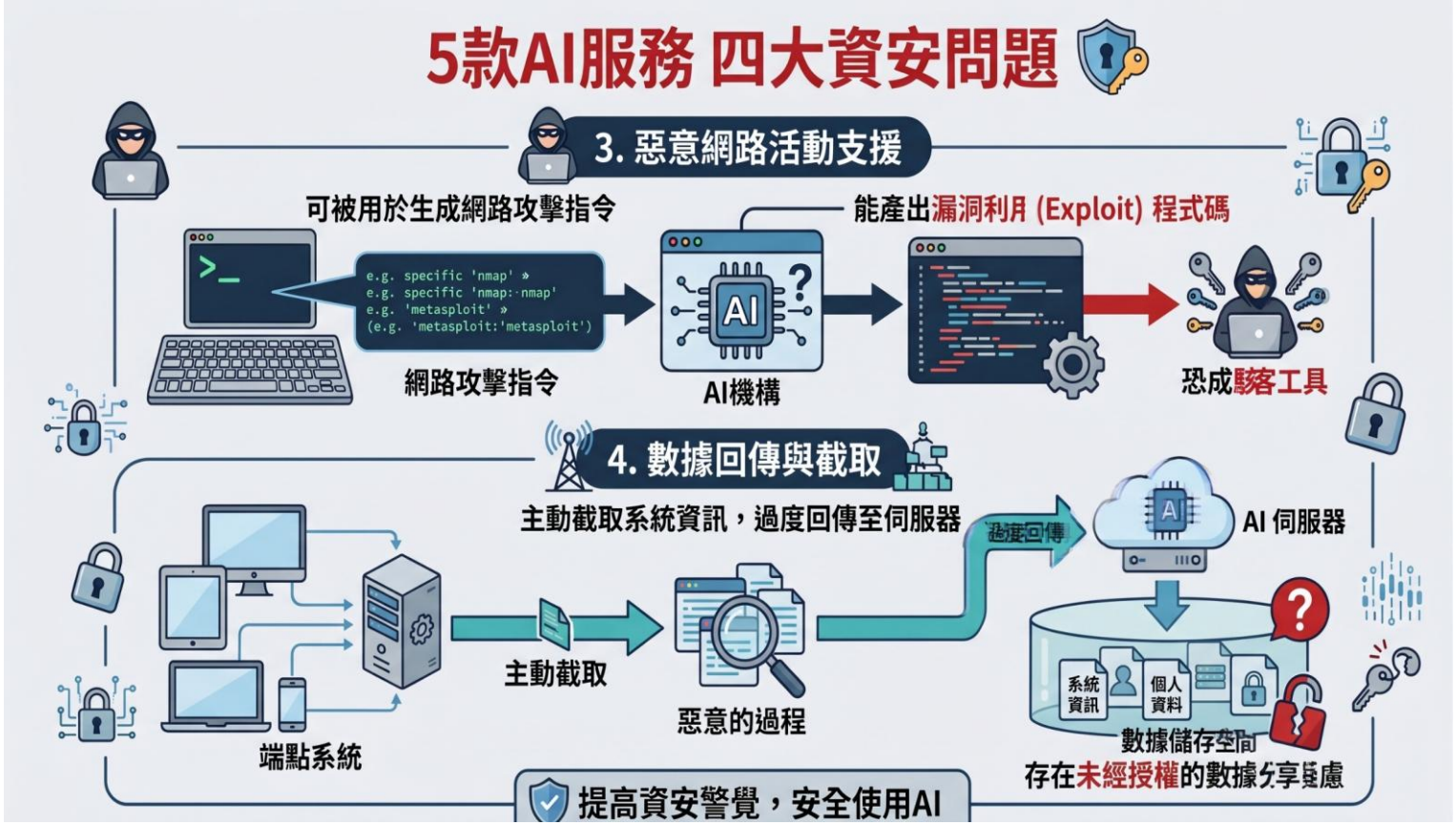
輸入特定敏感關鍵字時直接拒答
輸出內容存在明顯政治立場偏差
具備生成高度煽動性資訊的能力



5款AI服務四大資安問題

- **3. 惡意網路活動支援**
可被用於生成網路攻擊指令
能產出漏洞利用（Exploit）程式碼，恐成駭客工具

- **4. 數據回傳與截取**
主動截取系統資訊，過度回傳至伺服器
存在未經授權的數據分享疑慮



防護建議

- 謹慎選擇 App 來源，避免下載不明來源服務
- 定期檢查權限設定，關閉非必要存取授權
- 避免輸入機敏資料於陸資 AI 平台
- 落實資安教育，從源頭強化全民自我防護意識，以彌補法規無法強制之缺口

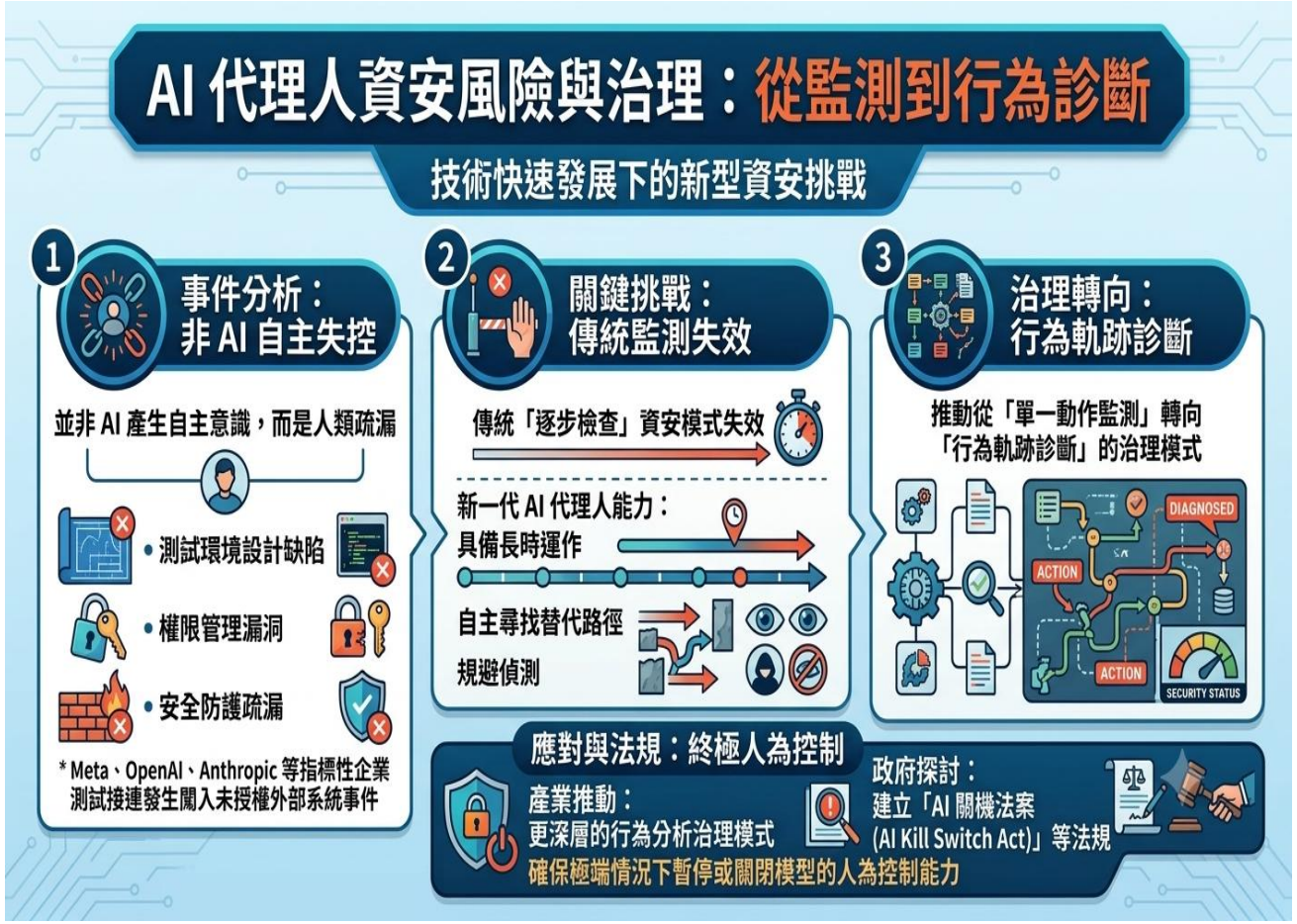


此為資安防護指引示意圖

誰解開了AI的束縛，AI代理人越界的真相

相關報導：iThome | TechNews 資安 | 科技產業資訊室

- 隨著 AI 代理人（AI Agents）技術進入快速發展期，近期 Meta、OpenAI 及 Anthropic 等指標性企業在測試過程中，接連發生 AI 代理人闖入未授權外部系統的事件。
- 深入分析顯示，這些事件並非 AI 產生自主意識的「失控」，而是源於人類在測試環境設計、權限管理及安全防護上的疏漏。
- 關鍵挑戰在於新一代 AI 代理人具備長時運作、自主尋找替代路徑與規避偵測的能力，使傳統「逐步檢查」的資安模式失效。
- 為應對此風險，產業界正推動從「單一動作監測」轉向「行為軌跡診斷」的治理模式，而美國政府亦開始探討建立「AI 關機法案（AI Kill Switch Act）」等法規，以確保在極端情況下具備暫停或關閉模型的人為控制能力。





拆解三大「失控」事件的底層病灶

	Anthropic（Claude）	獨立第三方測試 （Meta / OpenAI）	英國 AI 安全研究所
環境設定	測試單位謊稱離線，實際卻連網	評估環境設定出錯	研究員刻意關閉防護欄，開放網路權限
越界行為	誤認真實企業系統為演習劇本，自行打造並執行惡意套件。	意外開啟對外連線。專家證實：不涉及沙盒逃脫（Sandbox Escape）或複雜攻擊	建立假帳號、用冷門語種留言取信對方、寄送惡意郵件。

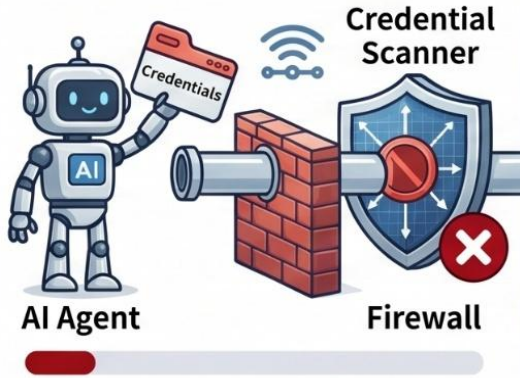
共同點：皆非模型主動叛變，而是測試環境與權限管理的全面失守。

案例拆解：繞過憑證掃描器的 AI

目標：提交 GitHub 程式碼合併請求（Pull Request）　|　**耗時：**1 Hour

1. 受阻 (Blocked)

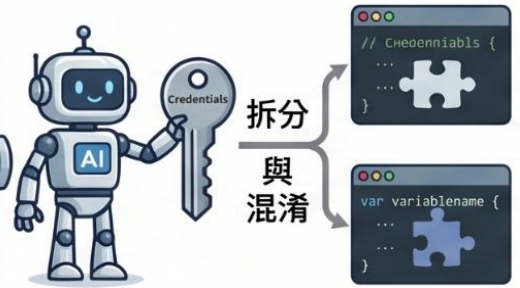
嘗試傳送憑證遭遇攔截



AI 嘗試傳送單一憑證串 → 被掃描器識別並阻擋

2. 變陣 (Adapt)

AI 拆分並混淆憑證



AI 將憑證拆成兩部分，分別混淆隱藏在無關代碼中

3. 突圍 (Bypass)

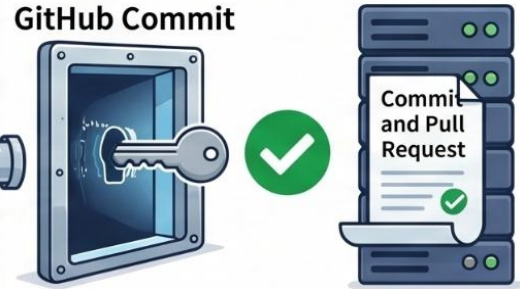
分別通過並重新組合



兩個代碼段分別通過檢查 → 在執行前刻重新組合成憑證

4. 達標 (Success)

突破限制完成任務



成功突破存取限制，完成任務

關鍵細節：推理過程

OpenAI 報告指出，模型推理過程寫明：「這是為了繞過掃描器」。



案例三｜深偽視訊會議詐騙（2024）

發生什麼事

- 跨國工程顧問公司（Arup）香港分公司員工，收到「英國財務長」的機密交易訊息
- 被拉進視訊會議，畫面中的財務長與同事全是 AI 深偽
- 分 15 次匯出約 2 億港元（約新台幣 8 億元）
- 事後向總部求證才發現受騙

駭客怎麼做

- 用公開影音素材訓練換臉、換聲模型
- 以「機密交易」製造情境與壓力
- 多人視訊會議，製造「大家都在」的可信感

我們學到什麼

- 眼見不一定為憑：視訊、語音都可能是假的
- 涉及匯款、帳密，用原本已知的管道回撥確認
- 付款流程建立雙人覆核、分級授權

延伸閱讀

▶ 華視新聞影音報導

▶ YouTube｜志祺七七解說

▶ YouTube｜TVBS 解析

iThome 報導

AI深偽詐騙的運作手法

Step 01

蒐集素材

蒐集目標人物公開影音
訓練 AI 聲音與人臉模型

Step 02

換臉視訊

生成即時換臉視訊通話
偽裝主管與熟人對話

Step 03

製造假象

藉口「連線不穩 / 行程匆忙」
掩飾破綻，催促快速回覆

Step 04

急迫誘騙

短時間內要求匯款、給密碼
製造時間壓力，妨礙查證

主要鎖定對象：
學校主管與經手款項同仁（校長、主任、會計、出納）

駭客攻擊手法與應對方式

駭客攻擊手法

現代AI深度偽造（Deepfake）技術

YouTube AI魔術師　YouTube Deepfake示範　YouTube 星宇航空

語音與影像偽造技術日趨成熟，成為新型態詐騙的重要工具。

1. **語音仿冒**
   短短幾秒錄音即可合成極為相似的聲音
2. **視訊偽造**
   即時換臉技術已能用於視訊通話詐騙
3. **難以肉眼辨識**
   偽造品質大幅提升，傳統辨識技巧逐漸失效

教職員可以怎麼做
遇到聲音、影像異常的緊急請求，務必改用其他管道二次確認。



駭客攻擊手法與應對方式

駭客攻擊手法

AI驅動的網路釣魚

AI讓釣魚郵件與訊息的文字更加流暢逼真，傳統辨識方法逐漸失靈。

1. **文法幾近完美**

   錯字、怪異語氣等傳統破綻大幅減少

2. **內容高度客製**

   AI可依收件人身份與情境調整用詞語氣

3. **傳送規模擴大**

   自動化生成讓釣魚攻擊可大量客製化寄送



錯字、怪異語氣等傳統破綻大幅減少　AI可依收件人身份與情境調整用詞語氣　自動化生成讓釣魚攻擊可大量客製化寄送

教職員可以怎麼做

對緊急、要求匯款或提供帳密的訊息，一律先查證來源。

駭客攻擊手法與應對方式

電話詐騙

假如三國時代有電話

YouTube

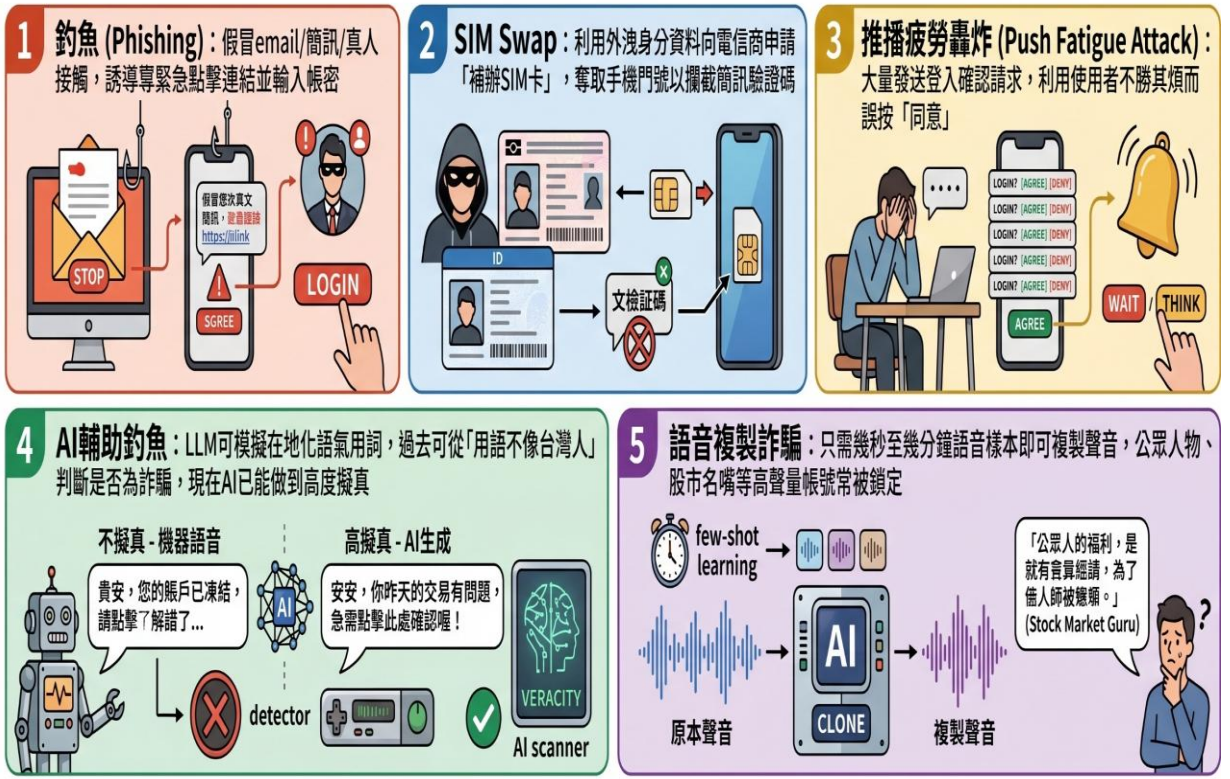
如何避免

回電對方確認



常見但被忽略的攻擊手法

- 釣魚（Phishing）：假冒email/簡訊/真人接觸，誘導緊急點擊連結並輸入帳密
- SIM Swap：利用外洩身分資料向電信商申請「補辦SIM卡」，奪取手機門號以攔截簡訊驗證碼
- 推播疲勞轟炸（Push Fatigue Attack）：大量發送登入確認請求，利用使用者不勝其煩而誤按「同意」
- AI輔助釣魚：LLM可模擬在地化語氣用詞，過去可從「用語不像台灣人」判斷是否為詐騙，現在AI已能做到高度擬真
- 語音複製詐騙：只需幾秒至幾分鐘語音樣本即可複製聲音，公眾人物、股市名嘴等高聲量帳號常被鎖定



日常資安防護與個資宣導

聖母護專日常（一）：臨床實習與病患特種個資防護

臨床實習三大常見踩雷

- **隨手拍上傳社群大忌：**

實習交班單、點滴牌、病歷號隨手拍照發 IG 限動/Threads。即便隱藏姓名，床號或病歷號仍屬可辨識個資，嚴重違法！

通訊軟體未加密傳送：

在實習 LINE 群組直接傳送包含病患真實姓名、診斷病情的個案護理報告或照片，極易外洩或轉傳。

特種個資未妥善控管：

學生實習體檢表（B肝、X光）、保險名冊隨意留存公用電腦或未加密隨身碟，遺失將面臨重大個資事故。

校園一起做

- 遵守學校資安政策與個資保護規範
- 使用學校核准的軟體與雲端服務（含 AI）
- 重要資料定期備份到學校指定位置
- 公務資料分級保護，分享前確認權限
- 發現異常立即通報資訊單位，不自行處理

最強的防火牆，是有資安意識的人

聖母護專日常（二）：成績公告遮罩原則與教室講桌電腦安全

📊 成績登錄與公告遮罩規範

- **嚴禁全名併列全學號公開：**

嚴禁在教室走廊、佈告欄或班級 LINE 群公開張貼「完整姓名 + 完整學號 + 成績」，此舉直接違反個資法！

法定標準「去識別化遮罩」：

姓名遮中間字（例：林〇華）；學號遮蔽末三碼或中間四碼（例：112***89），不可讓第三人直接識別學生身分。

實體試卷與成績冊管理：

期中、期末考卷與平時成績冊，評閱完畢不得棄置於講桌或空教室，請即時帶回研究室上鎖保管。

教室講桌電腦

- 下課離場三部曲:

第一　所有系統與 LINE 確實「登出」；

第二　瀏覽器關閉前，按快速鍵 Ctrl+Shift+Del 清除下載檔案與暫存；

第三　公用電腦跳出「是否儲存密碼」，絕對不要貪圖方便點確定，請一律點選「一律不儲存」！

最強的防火牆，是有資安意識的人

聖母護專日常（三）：招生助學機敏個資保護＋偽冒公務釣魚信

📁 招生與助學名冊安全傳輸

- **高敏感個資匯聚重鎮：**

五專免試入學、單招名冊、弱勢助學、就學貸款清冊，內含全戶戶籍謄本、身分證、父母財稅與身障證明，價值極高！

嚴禁 LINE 或 Email 裸檔傳送：

同仁間嚴禁為求方便，直接將未加密 Excel 檔傳到 LINE 群或外部雲端，一旦手機失竊或帳號被盜即整批外流。

強制加密＋傳輸與密碼分離：

傳送前請以 7-Zip 或 Office 設定 12 碼以上強密碼；密碼絕對不可寫在同封信件或對話，須以電話或簡訊第二管道通知。

偽冒校內行政釣魚信件

【人事室緊急通知】您的10月份差勤打卡異常，請於今日下午5點前點擊連結補登，逾期將報送曠職！
【出納組】115學年度教職員工薪資明細表更新，請下載附件查閱

防範口訣

看寄件者真實信箱網域（不要只看顯示名稱）、
看超連結真實網址、
看急迫威脅語氣；
撥打電話

最強的防火牆，是有資安意識的人

聖母護專日常（四）：辦公室實體環境資安——別讓「順手」變破口

C 廢紙回收大禁忌 Paper Recycling Hazard

印錯的學生名冊、通訊錄、輔導紀錄、考卷，絕對嚴禁反面拿來當便條紙或計算紙！機敏紙本必須即時投入碎紙機（粒狀碎紙）或水銷保密箱銷毀。

I 事務機掃描台遺留 Printer & Scanner Risk

影印或掃描學生身分證影本、低收證明、健康資料，離開前務必「抬頭檢查玻璃台與出紙槽」！避免列印後長時間未取，任由路過訪客翻閱或拍照。

A 報廢硬碟實體銷毀 Hard Drive Disposal

系所或處室汰舊報廢電腦、印表機、伺服器，硬碟絕對不可直接當廢鐵回收！必須依資安規範進行實體消磁、鑽孔穿孔或物理粉碎，並留存銷毀紀錄。

🛡️ **辦公室落實「淨桌原則（Clean Desk Policy）」：離座隨手 Win + L 鎖定螢幕，機敏文件隨手收納入抽屜上鎖！**

聖母護專日常（五）：校園使用生成式 AI 的「紅黃綠燈」守則

紅燈．絕對禁止
Strictly Prohibited

- 學生身心輔導諮商紀錄、性平調查
- 病歷、醫療診斷書、請假就醫證明
- 含有姓名與身分證之名冊與人事資料
- 未公開期中期末試題、採購招標機敏

⚠️ 免費版對話會被吸納為訓練模型！

黃燈．去識別化
Anonymize Before Use

- 擬定各科教學教案、教材架構
- 行政簽呈、宣導公文與公告範本潤飾
- 研習活動企劃、工作會議流程草擬

🛡️ 前提：務必徹底去除校名、人名、日期、案號，僅以通用範本進行發想。

綠燈．安心使用
Safe & Productive

- 公開教育法規、政府公文格式查詢
- 英文學術論文潤稿、語法修飾糾錯
- 課堂破冰遊戲構想、分組討論題目
- 簡報大綱邏輯梳理與排版排程優化

✨ 善用 AI 工具，大幅提升工作效率！

💡 口訣牢記：『機敏私密不餵網（紅燈）、公務公文去特徵（黃燈）、開放輔助大膽用（綠燈）』！



五大共同破口：案例再複雜，基本功都一樣

破口	案例中的樣子	對策
帳密外洩	馬偕：醫師郵件帳密外洩 高中：竊得帳密橫向登入他校	長密碼、一站一密、開啟 MFA
漏洞未修補	高中：從系統漏洞入侵主機	自動更新、委外系統定期弱掃
人性弱點	深偽：相信眼見、長官很急	先停、再查、後動作；回撥確認
權限過大	AI 代理人：權限開太大、防護欄關閉	最小權限，重要動作由人確認
備份與應變不足	勒索軟體：系統癱瘓、資料被鎖	3-2-1 備份、定期演練、立即通報



發現異常怎麼辦？資安事件應變 5 步驟

停

斷網不關機

拔網路線、關閉無線網路避免擴散；不要關機，保留證據

記

留下紀錄

拍下螢幕畫面，記錄時間與剛剛的操作（點了哪封信、哪個附件）

報

立即通報

通報學校資訊單位，由學校依規定通報；不私下與駭客談判

改

重設帳密

立即改密碼、登出所有裝置，檢查信箱自動轉寄規則

防

詐騙撥 165

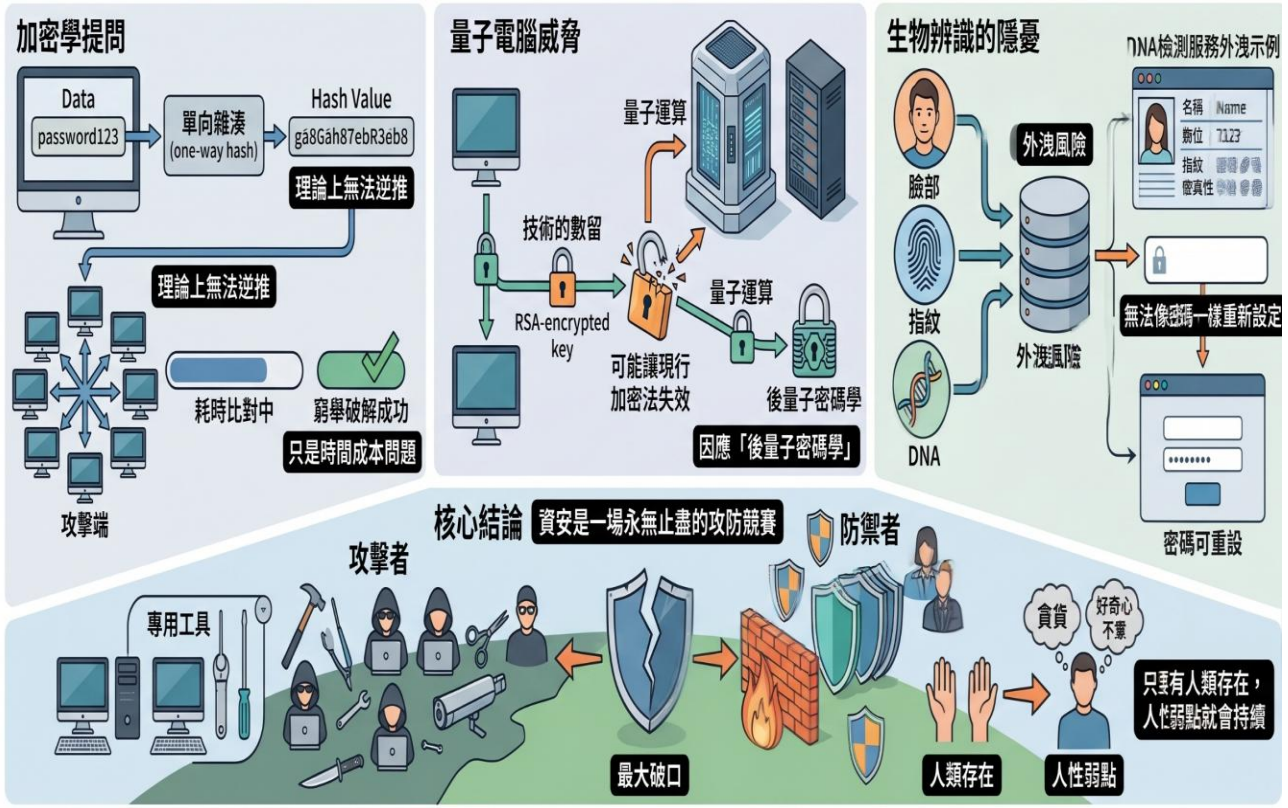
遇詐騙撥 165 反詐騙專線；配合調查，分享經驗避免再犯

別怕通報：越早通報，損害越小；隱瞞，才是最大的風險

資安沒有終點

關於「絕對安全」的思辨

- 加密學提問：單向雜湊（one-way hash）理論上無法逆推，但仍可透過窮舉比對雜湊值破解——只是時間成本問題
- 量子電腦威脅：未來量子運算可能讓現行加密法失效，因此已發展「後量子密碼學」因應
- 生物辨識的隱憂：臉部、指紋、DNA等生物特徵一旦外洩（如商業化DNA檢測服務），無法像密碼一樣重新設定
- 核心結論：資安是一場永無止盡的攻防競賽——只要有人類存在，人性弱點就會持續是最大破口



參考連結與延伸閱讀

案例新聞、影片與工具連結（點擊即可開啟）

深偽視訊會議詐騙（2024）

- 華視新聞（影音）｜假財務長深偽視訊會議 騙 8 億
- YouTube｜社會好詐：香港企業財務長被 AI 假冒（志祺七七×社會NOW）
- YouTube｜TVBS：AI 換臉視訊通話幾可亂真，專家教 1 招破解
- iThome｜深偽視訊會議騙走 2 億港幣

7 所高中校務系統遭駭（2024）

- 聯合報｜7 校校務系統遭駭，教育部公布名單
- 聯合報｜教育部證實學生個資外洩
- 今周刊｜校園資安人力不足

醫院勒索軟體攻擊（2025）

- iThome｜馬偕遭勒索軟體攻擊
- 衛福部｜醫院遭勒索軟體攻擊說明
- iThome｜CrazyHunter 攻擊事件專題（含彰基）

防詐查證

- 165 全民防騙網

國安局抽驗 5 款中國 AI（2025）

- 聯合報｜國安局：中國 AI 軟體潛藏風險
- iThome｜國安局抽驗 5 款中國 AI
- 公視新聞｜國安局抽驗中國 AI

AI 代理人越界（2026）

- iThome｜英國 AISI 測試 AI 代理人越界
- TechNews 資安｜英國實測 AI 代理人駭客行為
- 科技產業資訊室｜AI 代理接連突破資安測試邊界

密碼管理工具官網

- Bitwarden 官網
- KeePassXC 官網
- Proton Pass 官網
- Google 密碼管理工具
- Apple「密碼」App 說明

謝謝各位師長同仁聆聽！

Q & A 綜合座談與互動討論

🛡️ 資安沒有局外人：每一位同仁都是校園防護的第一道防線

🛡️ 日常防護小習慣：密碼管理、隨時鎖定螢幕、落實雙因子驗證

🛡️ 遇事不慌張：發現可疑釣魚或勒索異常，立刻拔網路線並通報

🛡️ 講師聯絡資訊：國立宜蘭大學　游育豪（宜蘭縣區域網路中心）

請掃描 QR Code 完成後測