日常網路使用者應注意的資訊安全

國立中央大學 柯皓翔

114年08月29日

center96@cc.ncu.edu.tw

$ whoami

國立中央大學 柯皓翔 專任人員

- 校園授權軟體異常排除
- 個資稽核及資安稽核
- 弱點掃描及改善建議
- 資安通報事件處理
- 個人資料管理系統主導稽核員 BS 10012:2017
- 資訊安全管理系統主導稽核員 ISO 27701:2019
- 隱私資訊管理系統主導稽核員 ISO 27001:2022
- Microsoft 365 認證：基本概念 MS-900
- Microsoft認證：Azure 基礎 AZ-900
- 資安院資訊安全概論、資安健診

center96@cc.ncu.edu.tw

資訊安全
Information Security

資訊安全是一個**針對資訊作業環境制度、架構、框架、管理、技術、稽核、遵循性、法令及法規**的複雜性議題。

今天將介基本觀念與相關防護技術，大綱如下：

- 資訊安全基本觀念
- 電子郵件社交工程與防範
- 認識加密勒索與預防
- 資料防護與備份
- 個資蒐集、管理與保護
- 密碼設定與存取原則
- 個人電腦安全性設定

資訊安全的目標

C
I
A

機密性	Confidentiality	只有被授權的適當人員，才能瀏覽(或取用)資料，①驗證 ②授權 ③加密。
完整性	Integrity	僅允許授權用戶更改資料，並且這些資料變化(新增、更改、刪除)將在各個方面得到一致的內容，例如：數位簽章。
可用性	Availability	資料與電腦設備(含網路)資源，將始終提供授權用戶存取，例如：重複建置、容錯移轉

資訊安全的攻擊者

外部攻擊者

- 競爭對手
- 駭客
  - Lamer / Script Kids
  - Ethical hacker
  - Cracker

內部攻擊者

- 粗心大意的員工
- 心生不滿的員工

資安攻擊的主要項目

- 台灣每週平均遭受4,182次攻擊
- **87%**的惡意程式，採用**電子郵件**方式傳送。
- **瀏覽網頁**被自動下載，或透過**USB散播**也有。

用戶端電腦設備

社交工程仍為主要手法，附件檔案多為Office、PDF、RAR/ZIP、ISO。

智慧型手機與平板設備

透過手機簡訊發送的URL下載APK方式，與原廠手機內建惡意程式。

IoT網路設備

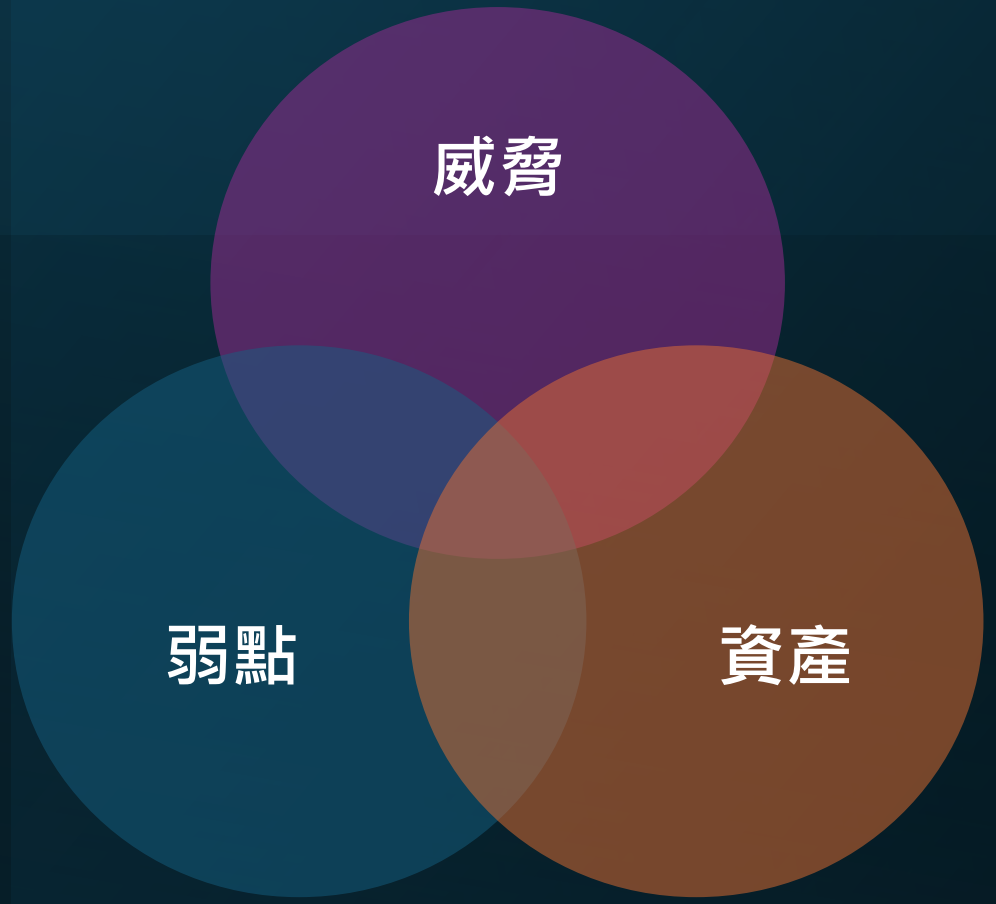
除了既有的CVE漏洞，預設密碼曝光也造成不小的危害。

網路主機與資料庫

未更新的漏洞修補，弱密碼，遠端桌面服務。

https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=11890

資訊安全的風險及風險管理



1、識別有哪些資訊資產

- 重要檔案、重要服務、哪個網路、哪個版本

2、評估資產的重要性

- 如果被破壞產生影響有多大？被偷改影響多大？

3、可能性

- 被破壞或被偷改的可能性是高還是低？

4、回應

- 緩解風險、接受風險、轉移風險、避免風險

5、監控

資訊安全如何落實

How to Prevent

- 程式設計漏洞
  - ✓修補漏洞，更新套件，使用正版軟體
- 系統設定疏失
  - ✓規範廠商，週期稽核
- 使用者不當行為
  - ✓教育訓練，資安演練

常見的攻擊手法

- 網路掃描與系統探測
- 竊聽網路通訊
- 遠端遙控
- 破解密碼
- 阻斷服務攻擊(DoS)
- 社交工程

社交工程
Social Engineering

甚麼是社交工程？

社交工程，是指以某種方式，博取陌生受害人的心理認同後，以進行資訊安全攻擊的手法，其某種方式可能是以電子郵件、語音電話、手機簡訊、偽冒網站等等手法。

常見的社交工程攻擊方式

- 垃圾式攻擊 Baiting Spam Mail Attack
- 水坑式攻擊 Watering Hole Attack
- 魚叉式攻擊 Spear Phishing Attack
- 釣魚式攻擊 Web/E-mail Phishing Attack

常見的用戶端攻擊模式

1. 垃圾式攻擊 Baiting Spam Mail Attack

- 垃圾式攻擊是以大規模廣播式方式發送釣魚郵件或廣告誘餌，不特定對象為目標，目的在於引誘使用者點擊連結、下載惡意程式或洩漏個資。

常見特徵

- 郵件主旨吸引眼球，可能包含**聳動**或**誘人**的社會時事，附有看似正常的連結或附件（例如 .docx、.zip、.pdf），常見寄件人偽冒如客服、銀行、宅配業者。

攻擊流程範例

- 寄出數千至數萬封郵件，等待少數受害者點擊，透過內嵌程式、連結、回覆要求收集資料或植入惡意軟體。
- 感染 Emotet、TrickBot、Lokibot 等 banking malware，適用於散播勒索軟體初期感染階段，常用於打開「第一道門」。

常見的用戶端攻擊模式

2. 水坑式攻擊 Watering Hole Attack

- 攻擊者鎖定某一特定組織或族群經常造訪的網站，先入侵該網站，植入惡意程式，等待「目標使用者」上鉤。

常見特徵

- 網站通常為政府網站、醫院網站、購物網站，一般使用者不會察覺網站已被竄改，惡意程式可能在後台進行 drive-by download，或要求更新安裝插件。

攻擊流程範例

- 偵測受害群常上之網站，入侵該網站，植入惡意碼，當受害者訪問，下載或被導向惡意伺服器。取得系統存取權限或種下後門。

常見的用戶端攻擊模式

3. 魚叉式攻擊 Spear Phishing Attack

- 此為針對特定對象、特定身份設計的詐騙行動，內容根據目標的背景、職務、習慣進行「高度客製化」，因此命中率極高。

常見特徵

- 郵件內容詳盡且個人化，例如稱呼姓名、公司名稱、工作項目。常冒充主管、HR、財務等內部單位。訊息語氣自然無破綻，甚至包含真實附件（如會議紀錄、採購單）。

攻擊流程範例

- 蒐集目標 LinkedIn、社群或公司網站資訊。撰寫客製化釣魚郵件。誘導目標點擊、下載、或輸入帳密。可用於進一步滲透（橫向移動、提權、部署勒索軟體）。

常見的用戶端攻擊模式

4. 釣魚式攻擊 Web/E-mail Phishing Attack

- 這是最普遍的社交工程攻擊形式。攻擊者**仿冒合法網站**（如銀行、電子郵件信箱入口、Apple ID），透過電子郵件或社群訊息誘騙使用者輸入個資、密碼、信用卡資料。

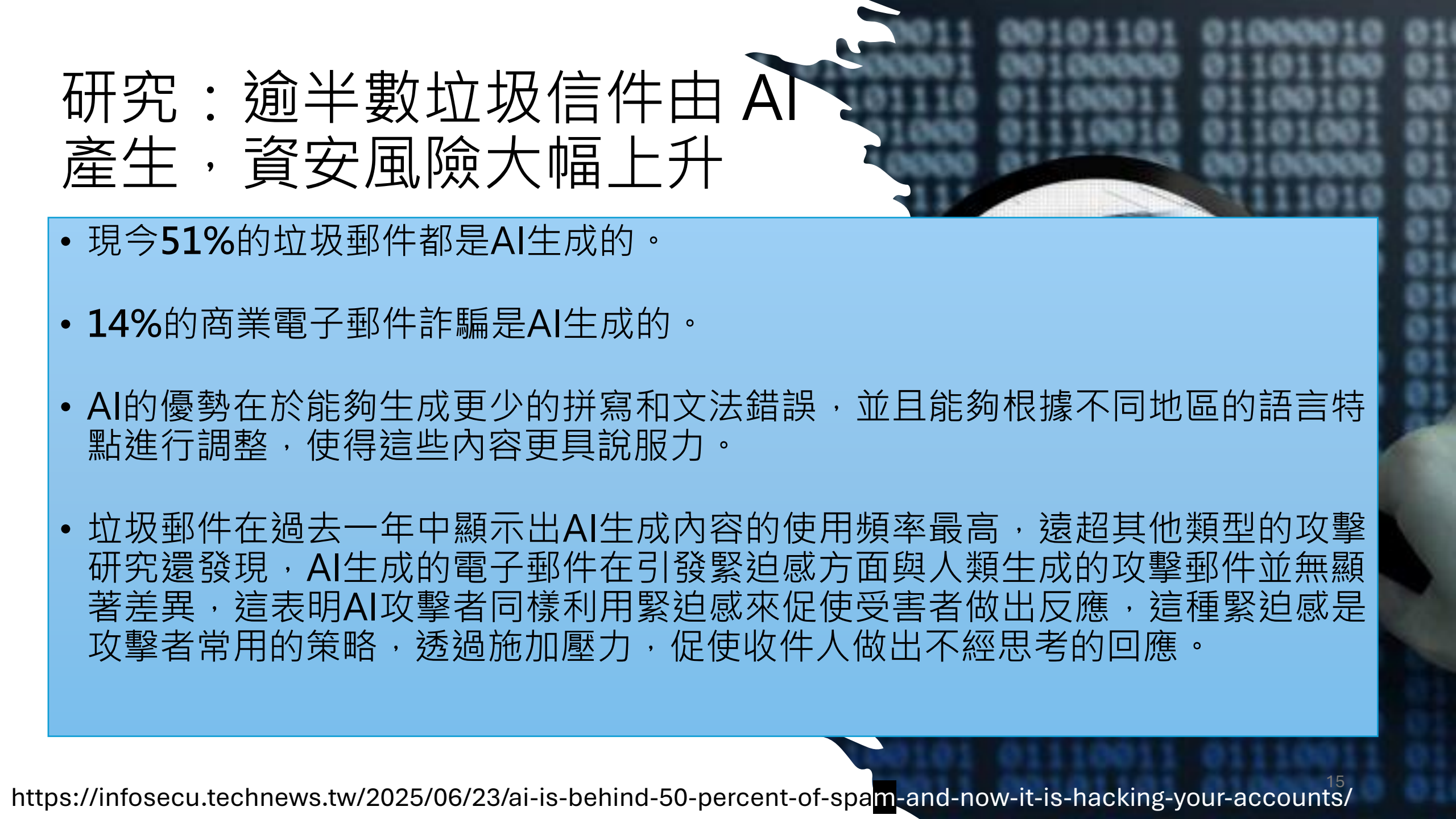
常見特徵

- 郵件偽裝為「系統更新」、「帳號異常登入」等通知，包含連結，導向高仿真網站登入頁，使用者輸入帳密後，資料會被直接截取。

攻擊流程範例

- 偽造信件＋釣魚網站，銀行帳單、信箱爆滿、快遞包裹

研究：逾半數垃圾信件由 AI 產生，資安風險大幅上升



- 現今51%的垃圾郵件都是AI生成的。
- 14%的商業電子郵件詐騙是AI生成的。
- AI的優勢在於能夠生成更少的拼寫和文法錯誤，並且能夠根據不同地區的語言特點進行調整，使得這些內容更具說服力。
- 垃圾郵件在過去一年中顯示出AI生成內容的使用頻率最高，遠超其他類型的攻擊研究還發現，AI生成的電子郵件在引發緊迫感方面與人類生成的攻擊郵件並無顯著差異，這表明AI攻擊者同樣利用緊迫感來促使受害者做出反應，這種緊迫感是攻擊者常用的策略，透過施加壓力，促使收件人做出不經思考的回應。

https://infosecu.technews.tw/2025/06/23/ai-is-behind-50-percent-of-spam-and-now-it-is-hacking-your-accounts/

偽冒網址網站的案例

- 偽冒網址：利用英數字的相近(O與0, l與1, w與vv, m與rn, C與G, q與9, 等等)
- 偽冒網站：利用網址的管轄差異(.com.tw與.com.tv .com.cn .com.ch .com.cz)

正確網站網址	偽冒網站網址	
www.cathaybk.com.tw	www.cathay-bk.com	金融銀行
www.taishinbank.com.tw	www.taishinz.com	金融銀行
www.bot.com.tw	www.bot-bank.com	台灣銀行
www.post.gov.tw	www.ipost-tw.com	中華郵政
webmail.tku.edu.tw	webmail.tku.eud.tw	大學電郵
www.chinatrust.com.tw	www.chinatnust.com.tw	金融銀行
tw.bid.yahoo.com	tw.bid.yah00.com	拍賣網站
www.landbank.com.tw	www.1and.com.tw	金融銀行
www.china-airlane.com.tw	www.china-air1lin.com.tw	航空公司
www.google.com.tw	www.goog1e.com.tw	網路服務
www.outlook.com	www.0utlook.com	電郵服務
www.microsoft.com	www.microosoft.com, www.rnicrosoft.com	軟體公司

偽冒網址網站的案例－Line 下載

利用搜尋引擎SEO機制提升排名

社交工程測試演練

對於防災防火防汛來講，所有安全演練，其目標都是要加強安全防護意識，**降低意外災害損失**，**提高員工危機意識**。

資訊安全的電子郵件社交工程攻擊與防護，定期透過各種測試演練，提供資安防衛能力，找出可能存在的弱點漏洞，事先演練，事先預防。

◆基本認識

- 模擬攻擊者透過電郵社交工程方式，取得被害人的個人資訊、金融資料與敏感檔案。

◆測試目標

1. 測試機構員工是否可能開啟駭客**電子郵件**
2. 測試機構員工開啟電子郵件**附件檔案**的危險行為比例
3. 測試機構員工點選電子郵件內文的**URL超連結**行為比例

◆防範方式

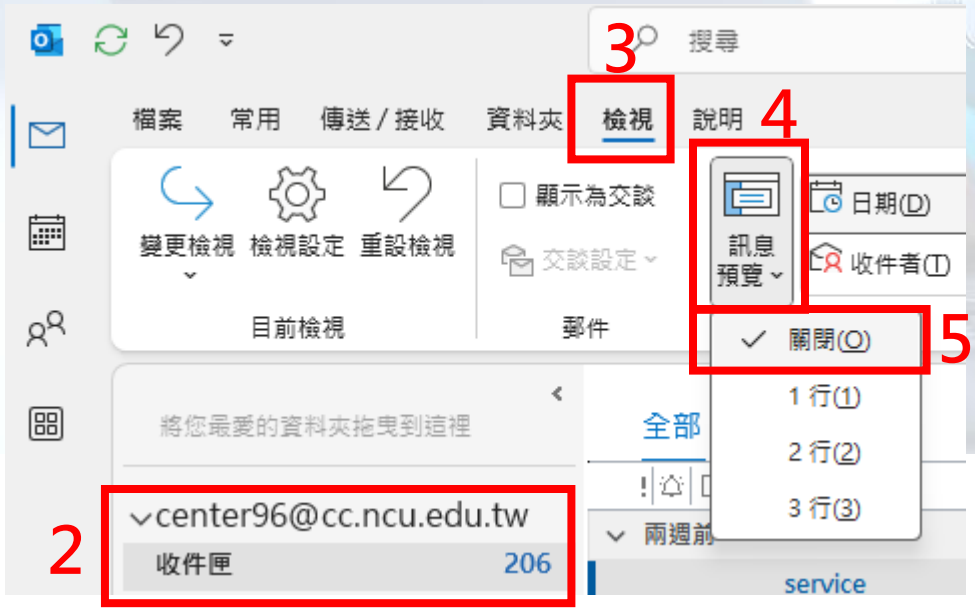
1. 電子郵件要關閉HTML預覽功能，用純文字瀏覽
2. 不要開啟**標題聳動**的電子郵件（休閒養生、薪資調整、疫情通知、折扣優惠等等）
3. 公務電子郵件信箱，不要點擊開啟**非公務郵件**

電子郵件安全性設定

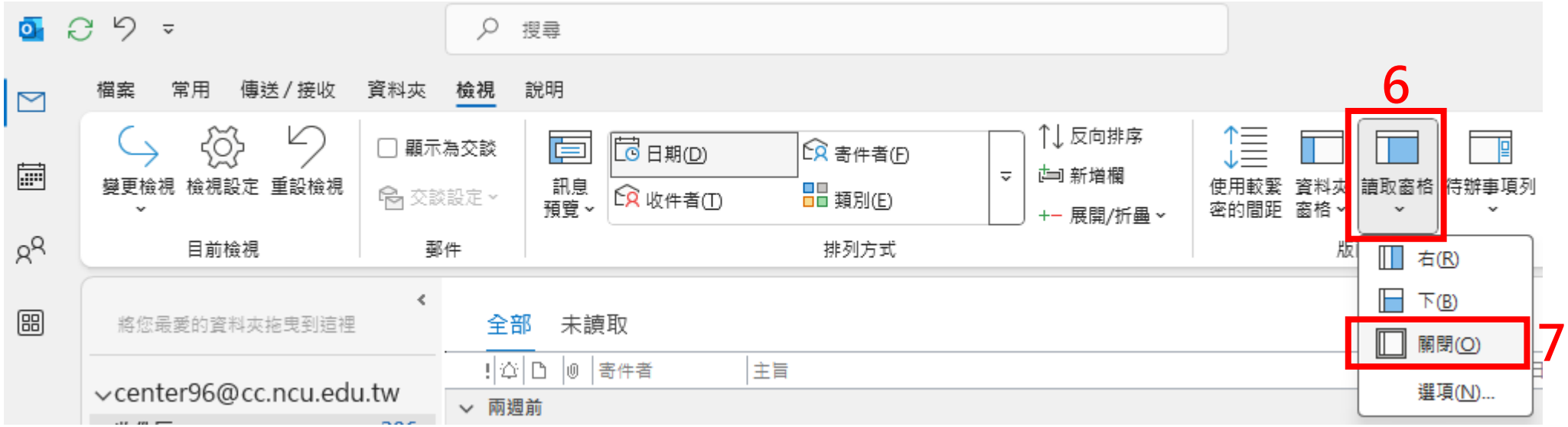
以 Outlook、Gmail、iOS、MAC OS 內建郵件為例，設定：

1. 關閉信件預覽功能
2. 關閉自動下載圖片
3. 以純文字讀取郵件
4. 不要自動回覆讀信回條

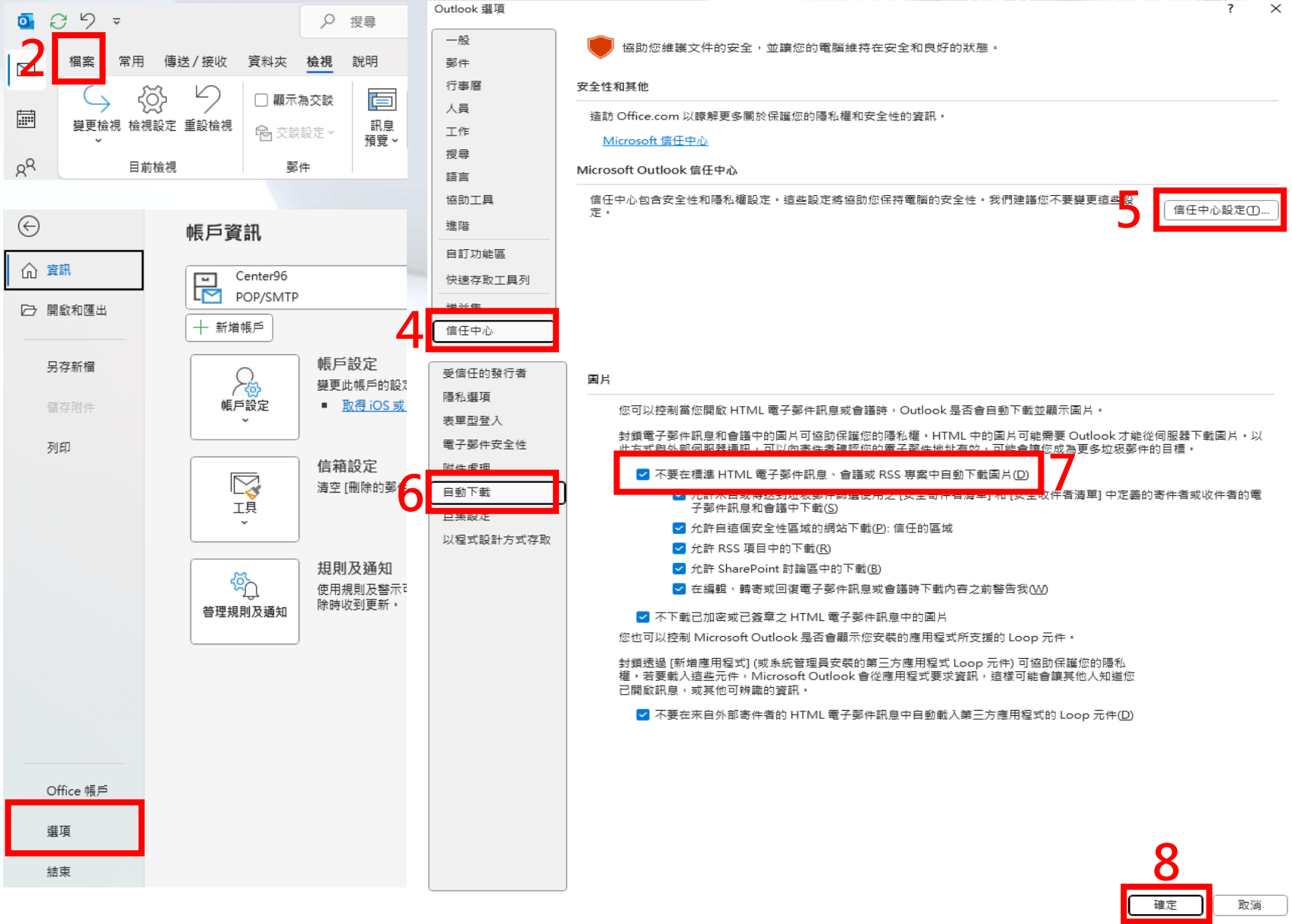
Outlook - 關閉信箱預覽功能



1. 開啟Microsoft Outlook
2. 點選收件匣
3. 點選【檢視】
4. 點選【訊息預覽】
5. 點選【關閉】
6. 點選【讀取窗格】
7. 點選【關閉】

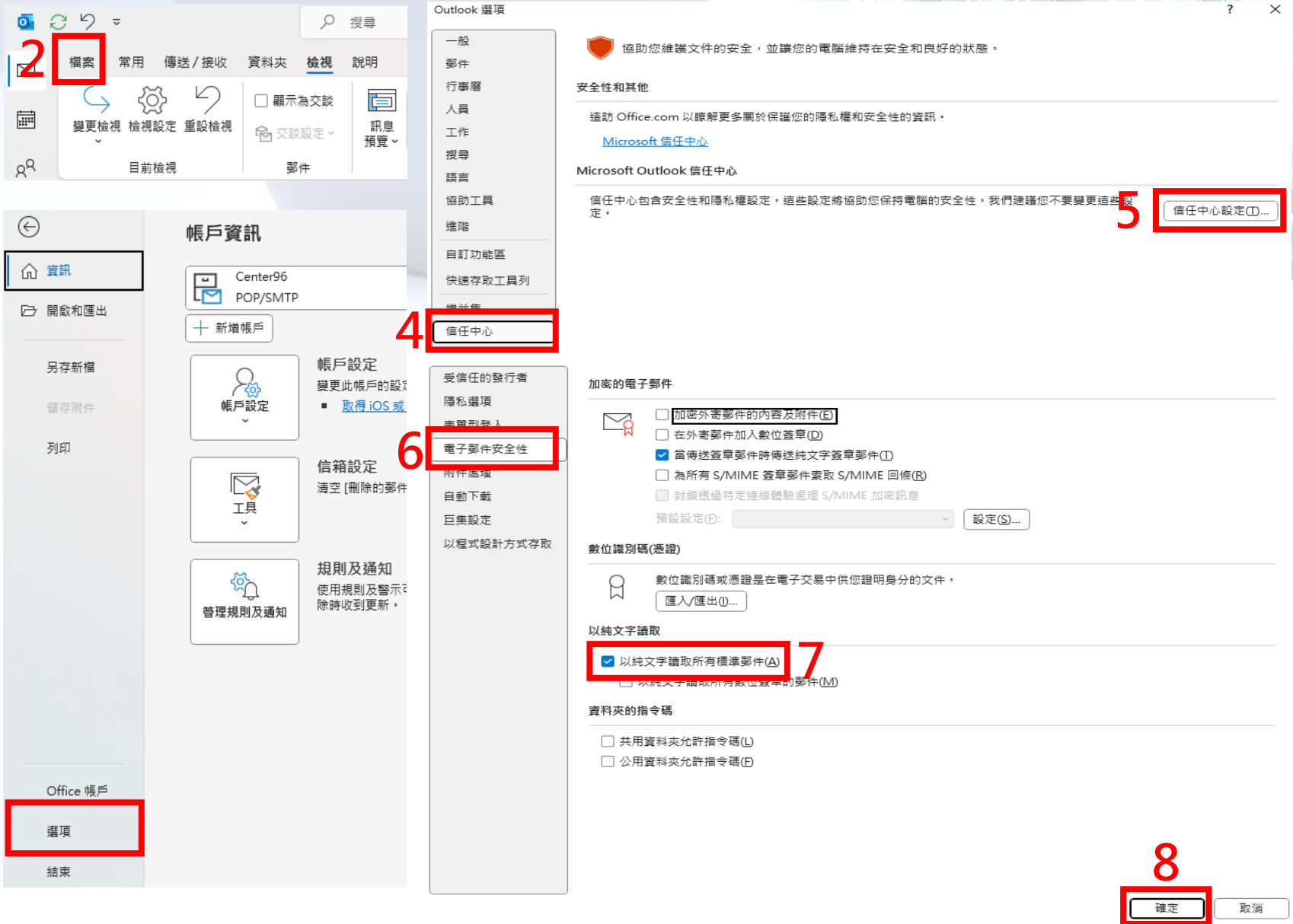


Outlook - 關閉自動下載圖片



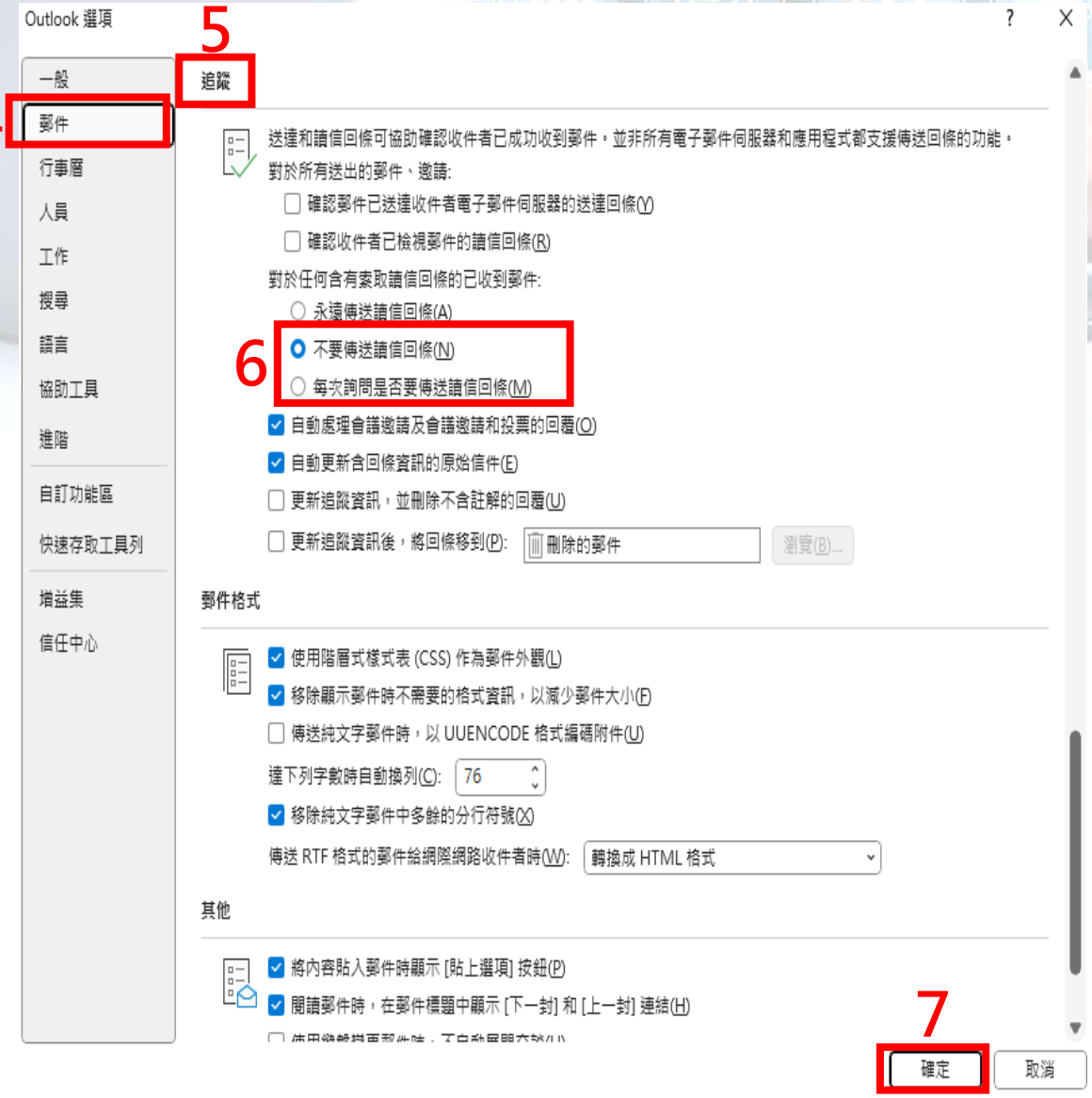
1. 開啟Microsoft Outlook
2. 點選【檔案】
3. 點選【選項】
4. 點選【信任中心】
5. 點選【信任中心設定】
6. 點選【自動下載】
7. 勾選【不自動下載 HTML 電子郵件訊息或RSS項目中的圖片】
8. 點選【確定】

Outlook - 以純文字讀取郵件



1. 開啟Microsoft Outlook
2. 點選【檔案】
3. 點選【選項】
4. 點選【信任中心】
5. 點選【信任中心設定】
6. 點選【電子郵件安全性】
7. 勾選【以純文字讀取所有標準郵件】
8. 點選【確定】

Outlook - 不自動回覆讀信回條

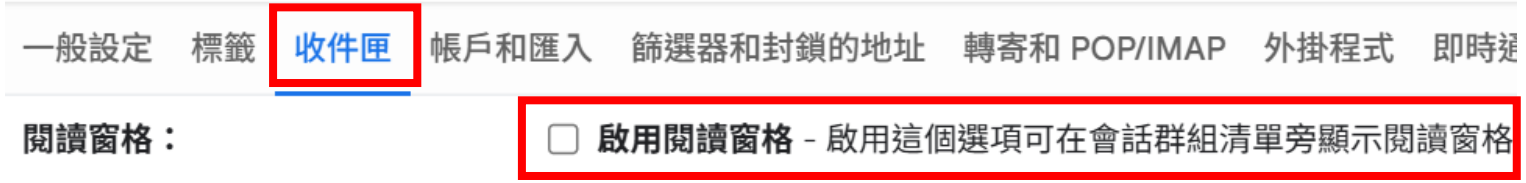


1. 開啟Microsoft Outlook
2. 點選【檔案】
3. 點選【選項】
4. 點選【郵件】
5. 移動上下垂直捲軸，找尋【追蹤】區塊
6. 勾選【不要傳送讀信回條】或是【每次詢問是否要傳送讀信回條】
7. 點選【確定】

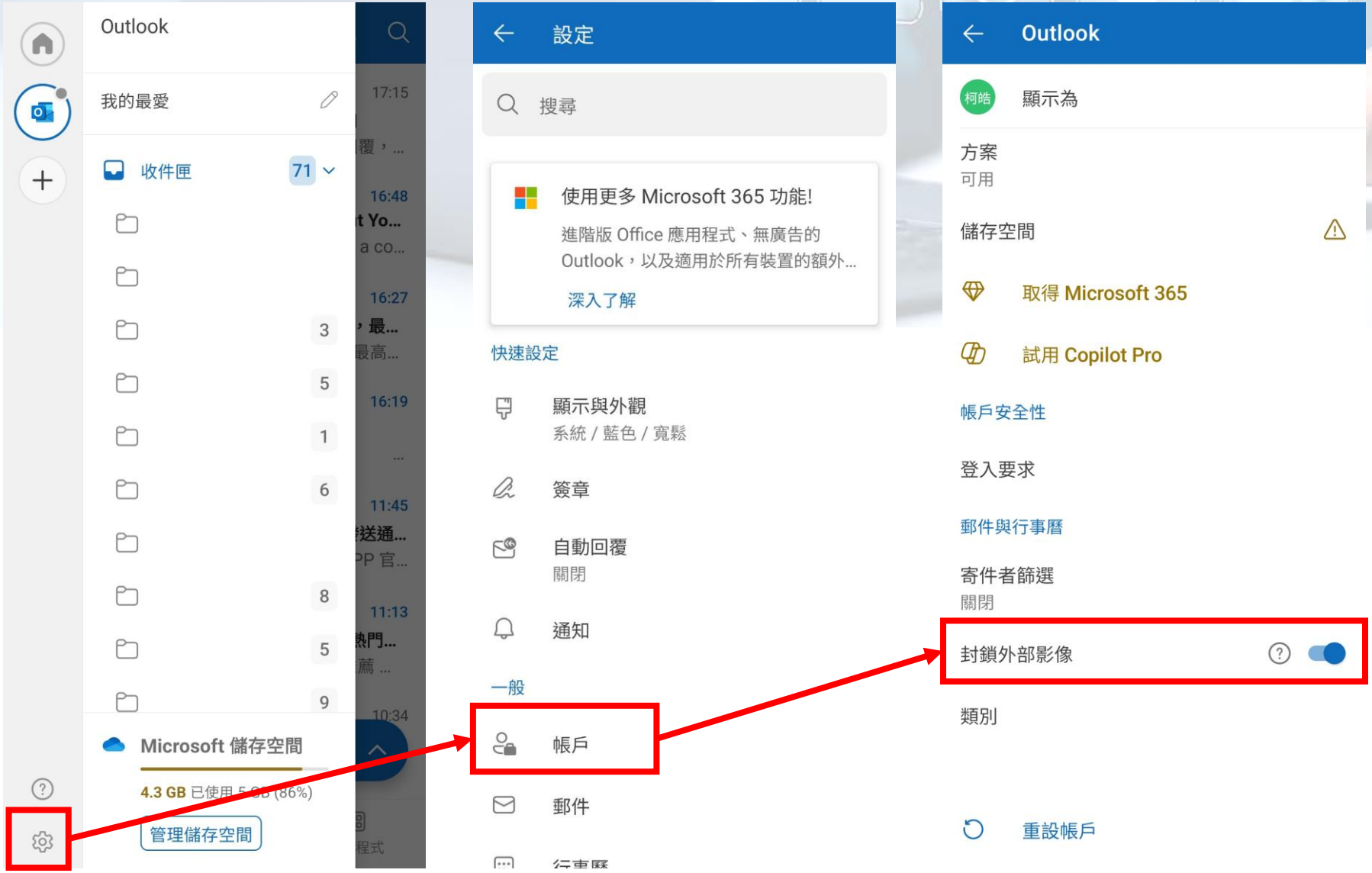
Gmail - 關閉信箱預覽及自動下載圖片

1. 關閉圖片自動下載功能

2. 關閉信件預覽功能

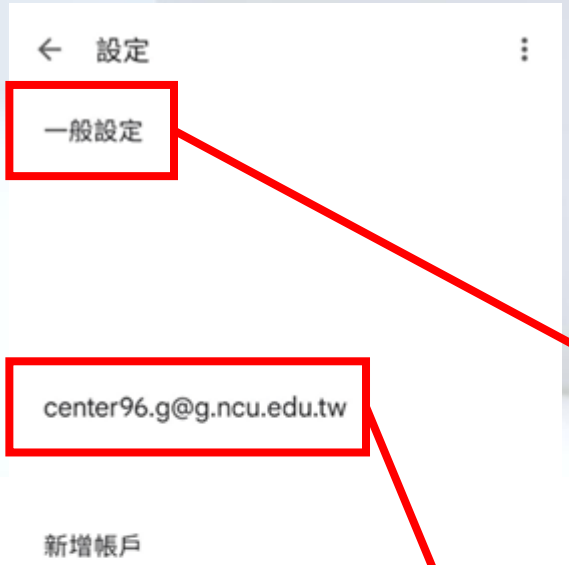


Outlook App - 關閉自動下載圖片



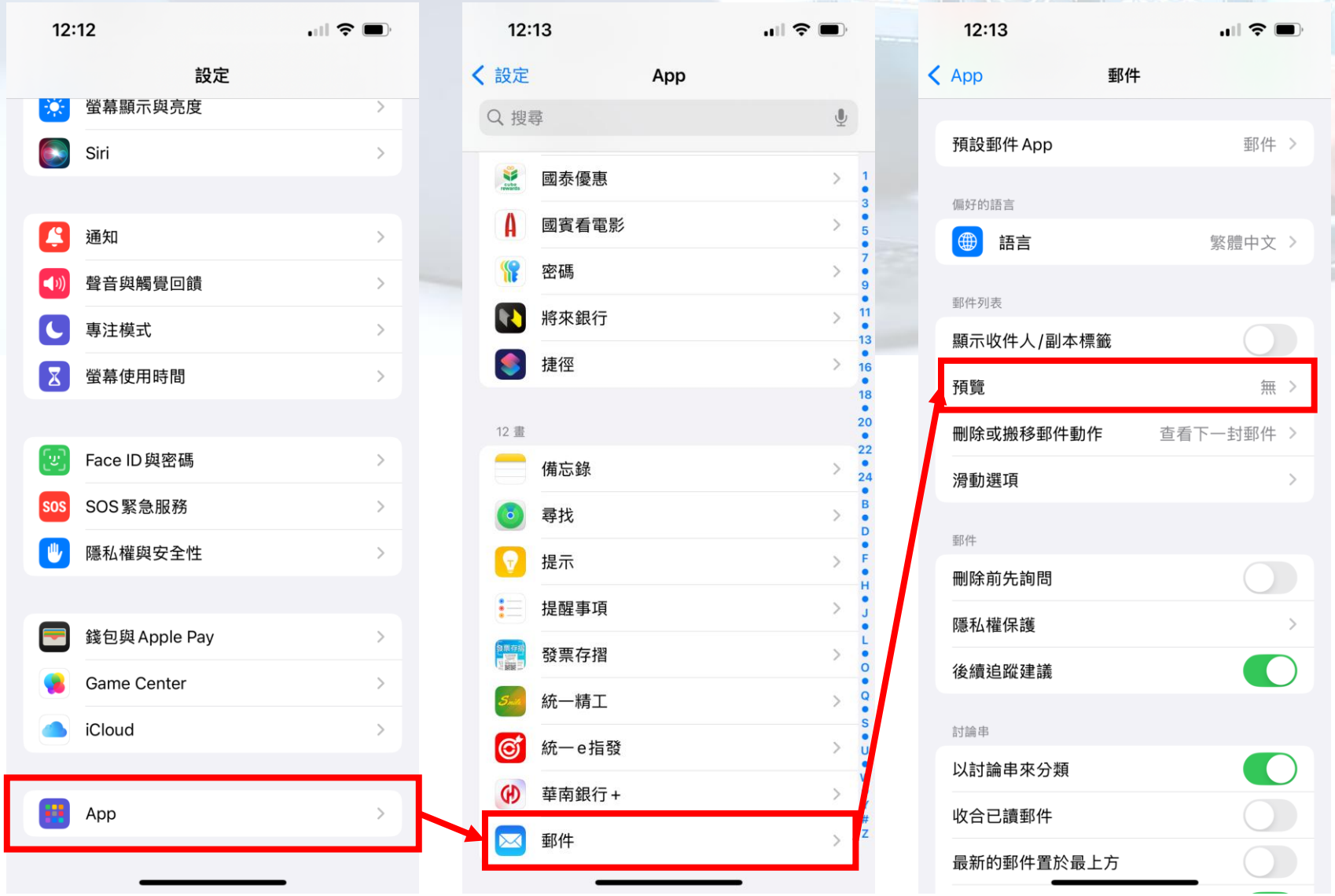
1. 請點選您的帳號
2. 將【封鎖外部影像】切換開關移至開啟

Gmail App - 關閉信箱預覽及自動下載圖片



1. 請點選您的帳號
2. 將【圖片】 選項選擇顯示不明外部圖片時，必須先詢問我。
3. 點選一般設定
4. 將【會話群組清單密度】更改為密集。

iPhone/iPad – 關閉信箱預覽

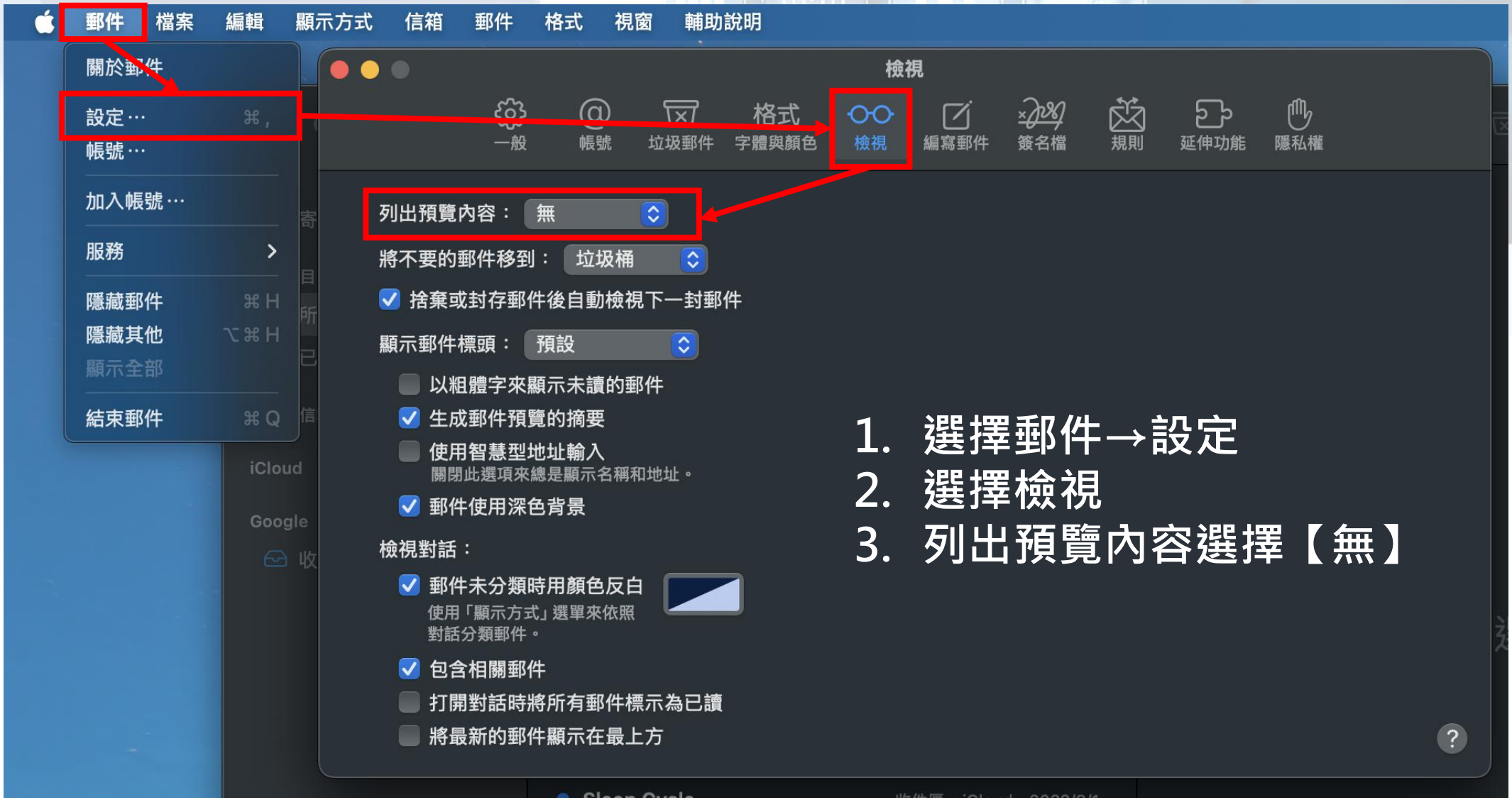


1. 選擇設定 → App
2. 找到「郵件」
3. 郵件列表的預覽選擇【無】

iPhone/iPad – 隱私權保護設定

1. 選擇設定 → App
2. 找到「郵件」
3. 找到「隱私權保護」
4. 開啟「隱藏IP位址」及「阻擋所有遠端內容」。

MAC –關閉信箱預覽


郵件
檔案
編輯
顯示方式
信箱
郵件
格式
視窗
輔助說明
關於郵件
設定⋯ ⌘,
帳號⋯
加入帳號⋯
服務
隱藏郵件 ⌘H
隱藏其他 ⌥⌘H
顯示全部
結束郵件 ⌘Q
檢視
一般
帳號
垃圾郵件
字體與顏色
檢視
編寫郵件
簽名檔
規則
延伸功能
隱私權
列出預覽內容： 無
將不要的郵件移到： 垃圾桶
捨棄或封存郵件後自動檢視下一封郵件
顯示郵件標頭： 預設
以粗體字來顯示未讀的郵件
生成郵件預覽的摘要
使用智慧型地址輸入
關閉此選項來總是顯示名稱和地址。
郵件使用深色背景
檢視對話：
郵件未分類時用顏色反白
使用「顯示方式」選單來依照對話分類郵件。
包含相關郵件
打開對話時將所有郵件標示為已讀
將最新的郵件顯示在最上方
iCloud
Google
1. 選擇郵件→設定
2. 選擇檢視
3. 列出預覽內容選擇【無】

MAC – 隱私權保護設定

1. 選擇郵件→設定
2. 選擇隱私權
3. 不要勾選【保護郵件活動】
4. 勾選【隱藏IP位址】及【阻擋所有遠端內容】

謠言澄清、詐騙破解 - MyGoPen

- https://www.mygopen.com/

密碼的破解方式

- 暴力式密碼攻擊
- 字典式密碼攻擊
- 電郵社交工程（惡意程式）
- 簡單密碼猜測（密碼潑灑攻擊）
- 密碼撞庫攻擊（憑證填充）

檢測自身帳號密碼是否外洩

檢測自身帳號密碼是否外洩

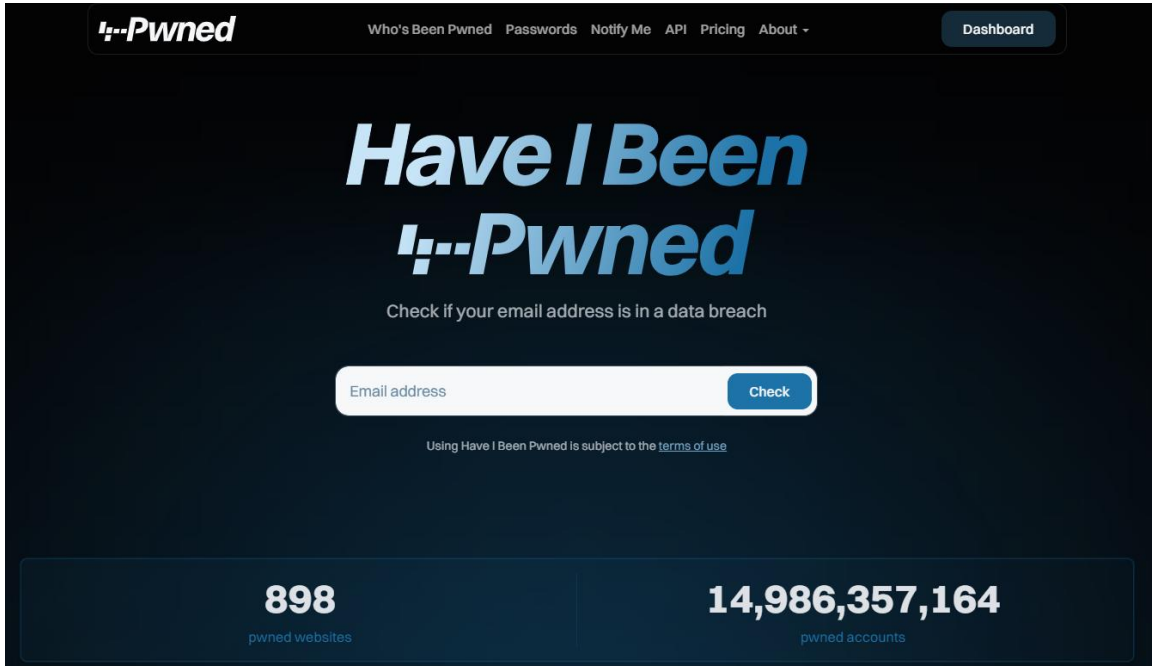
有無外洩？

➢沒有外洩
- 保持帳號密碼安全設定與習慣

➢有外洩
- 那些帳號
- 何時外洩
- 影響層面
- 根據以上三個要素，調整帳號密碼

檢測自身帳號密碼是否外洩 - HIBP

https://haveibeenpwned.com/



[註] 此處不要輸入公務用聯絡信箱

檢測自身帳號密碼是否外洩 – HIBP 結果

洩漏來源

Source

- 確認使否使用與目前金融服務相同的帳號名稱
- 確認是否使用相同密碼

洩漏日期

Time

- 該日期過後，是否繼續使用這組密碼
- 該日期過後，有無發生系統異常登入

洩漏資料

Compromised

- 該外洩資料類型是否關連到金融服務
- 該外洩資料是否為其他金融服務的備援信箱

洩漏影響

Effect

- 變更電子郵件資料的影響層面有多大
- 停用帳號的影響有多大

密碼設定與存取原則

1. **密碼足夠長且複雜**
   - 密碼的長度比複雜度更重要
   - 建議至少12–16字元，或用「密碼片語」
   - 禁止使用通用型態的密碼，例如：12345678、手機號碼、1qaz2wsx、ji32k7au4a83
   - 不要用關聯帳號的密碼，例如：

     帳號: jason1122@gmail.com → 密碼: 1122jason
2. **開啟多因素驗證**
   - 就算密碼外洩，駭客也無法輕易登入
3. **一旦懷疑外洩，就立即更換**
   - 不是無條件的定期更換
4. **登入主機的遠端桌面或遠端遙控需限定存取位址**
   - 遠距設備與主機服務，停用預設帳號密碼
   - 非約定時間，禁止廠商帳號遠端登入
   - 廠商員工離職後，需變更遠端登入的維護密碼
   - 維護廠商的不同員工，不要使用相同密碼遠端登入

惡意程式常見種類及散播方法

惡意程式

- Malware = Malicious Software

惡意程式的種類

- 電腦病毒
- 特洛伊木馬
- 電腦蠕蟲
- 傀儡網路
- 間諜程式
- 加密勒索

散播方法

- 透過網路
- 電子郵件
- USB隨身碟
- 瀏覽網頁

認識加密勒索

入侵

- 使用者操作行為
- 遠端登入或漏洞

加密

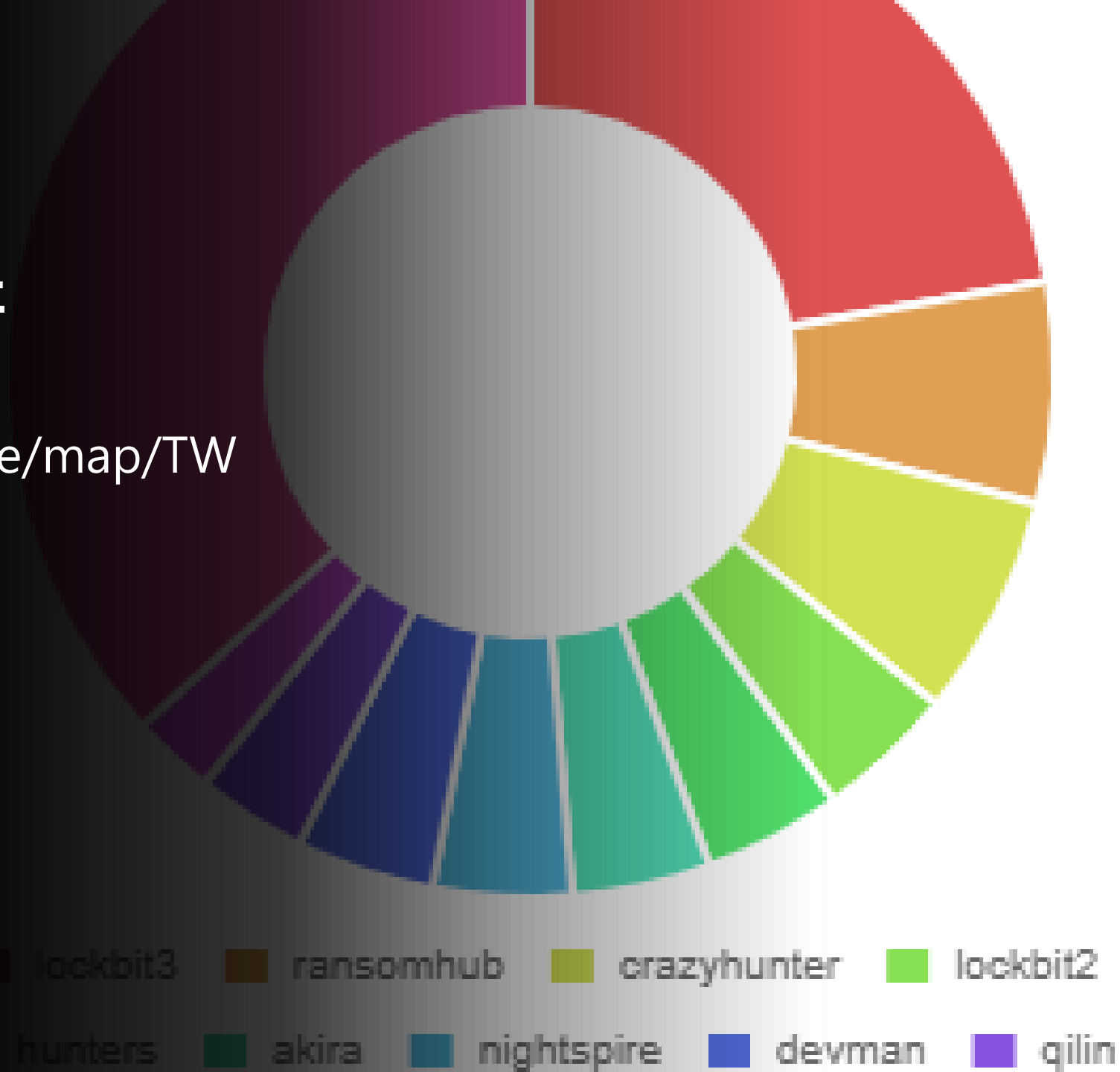
- Office Files (.doc, .docx, .xls, .xlsx, .ppt, .pptx, …)
- 圖片檔案
- 資料庫檔案

勒索

- TOR(暗網)
- Secure Mail
- Cryptocurrency

加密勒索近期案件

https://www.ransomware.live/map/TW



加密勒索背後龐大的不法利益

新聞：GandCrab勒索軟體賺了20億美元後宣佈收山 2019-06-03

https://www.ithome.com.tw/news/131042

加密勒索的處理策略
with in 72 hours

在報請調查單位與主管機關的同時，請先決定下列因應策略：

(0) 防堵社交工程、系統漏洞

(1) 資料檔案備份還原

(2) 電腦系統重新安裝（重灌）

(3) 支付贖金，救回資料（Risk）

(4) 不付贖金，等待解藥（至少一年以上）

資料檔案備份 3-2-1 原則

- 避免遭受加密勒索攻擊
  - 社交工程仍佔多數。
- 哪些檔案需要備份？
  - 定期備份檔案時，從外部取得的檔案，盡量不要備份(不一定是安全的)。
- 自主業務檔案備份
  - 每週或每月備份工作檔案成**3**份。
- 備份檔案儲存方式
  - 外接硬碟、 USB隨身碟、光碟、雲端硬碟、網路儲存設備(NAS)等等，至少用**2**種不同的方式儲存，**1**份離線且異地保存。
- 妥善保護備份檔案
  - 備份檔案要妥善置放於安全處，並且加密上鎖。
  - 重要資料檔案上密碼，可阻止攻擊者轉售竊取資料。

行動裝置的安全隱憂

1. 根據資安公司卡巴斯基（Kaspersky）發布的報告，2024年針對智慧型手機的惡意程式攻擊總數超過 3,330 萬次。

2. 在所有惡意程式類型中，針對手機銀行帳戶的木馬程式攻擊是增長最快的類別之一。
   - 有報告指出，這類攻擊在 2024 年成長了將近 200%，攻擊者正在改變策略，透過大規模散布惡意軟體來竊取金融憑證。

3. 以下是一些影響手機是否容易中惡意程式的因素：
   - 系統版本
   - 應用程式來源
   - 點擊可疑連結
   - 應用程式權限

行動裝置資訊安全 - Android

- Android 12 以前已經停止安全性更新
- 建議使用者將裝置**升級至 Android 13 或更新版本**，以確保安全性。
- 確認裝置的 Android 版本：
  - 前往**「設定」→「關於手機」→「Android 版本」**，
  - 查看您的裝置目前運行的 Android 版本。
- 檢查安全性更新：
  - 前往「設定」→「系統」→「更新」，
  - 查看是否有可用的安全性更新。
- 考慮升級裝置：若您的裝置無法升級至 Android 13 或更新版本，建議考慮更換支援更新的裝置，以確保資訊安全。

行動裝置資訊安全 – iPhone (iOS)

- iOS 16.7.7 以前已經停止安全性更新
- 建議使用者將裝置**升級至 iOS 17 或更新版本**，以確保安全性。
- 確認裝置的 iOS 版本：
  - 前往**「設定」→「一般」→「關於本機」**，
  - 您會看到「iOS 版本」這一欄，顯示目前您裝置的 iOS 版本號碼。
- 升級至最新版本的 iOS：
  - 前往「設定」→「一般」→「軟體更新」，
  - 檢查是否有可用的更新。

個人資料保護

- 自然人（民眾）
- 姓名、出生年月日、身分證字號
- 特徵、指紋
- 婚姻、家庭
- 教育、職業
- 健康、病例
- 財務情況、社會活動
- 其他**足以識別該個人之資料**。

防止個人資料被竊取、竄改、毀損或洩漏。

可能面臨的損害賠償責任

依照《個資法》第28條負損害賠償責任

1. 公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。
2. 被害人雖非財產上之損害，亦得請求賠償相當之金額；其名譽被侵害者，並得請求為回復名譽之適當處分。
3. 依前二項情形，如被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，以**每人每一事件新臺幣五百元以上二萬元以下**計算。
4. 對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害賠償者，其合計**最高總額以新臺幣二億元**為限。但因該原因**事實所涉利益超過新臺幣二億元者，以該所涉利益為限**。
5. 同一原因事實造成之損害總額逾前項金額時，被害人所受賠償金額，不受第三項所定每人每一事件最低賠償金額新臺幣五百元之限制。
6. 第二項請求權，不得讓與或繼承。但以金額賠償之請求權已依契約承諾或已起訴者，不在此限。

個資外洩的疑慮 – ChatGPT

[新聞] 這5類訊息不要跟ChatGPT說，一句話毀掉你的財產！這招保個資不外洩 2025-08-08

使用ChatGPT等AI要小心！5種資訊千萬別告訴AI
一、身份資訊
二、醫療資訊
三、財務資訊
四、登入憑證
五、公司機密

開啟這3大功能，保護你的對話與隱私
1. 關閉「改善模型」權限
2. 使用「臨時交談」功能
3. 提出「個資刪除」請求

https://www.edh.tw/article/38356

ChatGPT隱私設定 - 關閉「改善模型」權限

ChatGPT隱私設定 - 提出「個資刪除」請求

OpenAI隱私權中心 https://privacy.openai.com/

個人電腦安全性設定

- 家用電腦與辦公筆電的系統，需用正版並更新
- 要啟用Windows Defender，或安裝防毒軟體
- 公務相關檔案 (Office files) 存檔要用密碼加密
- 建議使用VPN線路進行遠距辦公(安裝VPN-Client)
- 不要開啟公務無關的電郵附件檔案，也不要下載安裝非授權的網路免費軟體
- 避免被加密勒索，絕對要落實備份檔案3-2-1原則
- 檔案備份後，備份設備需移除USB連線與網路連線

VIRUSTOTAL – 開源線上惡意程式檢測服務

- https://www.virustotal.com/

[註] 不要上傳帶有個資、需保密、個人金融資訊相關的檔案。