電子郵件社交工程及信箱安全性設定

國立政治大學 電子計算機中心 郭紫玫技士

2023.03

社交工程 Social Engineering

利用人性弱點，應用簡單的溝通和欺騙技倆，以獲取帳號、通行碼、身分證號碼或其他機敏資料，來突破校園的資通安全防護，遂行其非法的存取、破壞行為。

網路釣魚

誘騙使用者登入偽裝之網站以騙取帳號及通行碼等機敏資料。

垃圾郵件

利用電子郵件誘騙使用者開啟檔案、圖片或連結，以植入惡意程式、暗中收集機敏性資料。

不明的軟體

利用提供工具、檔案、圖片為幌子，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、暗中收集機敏性資料。

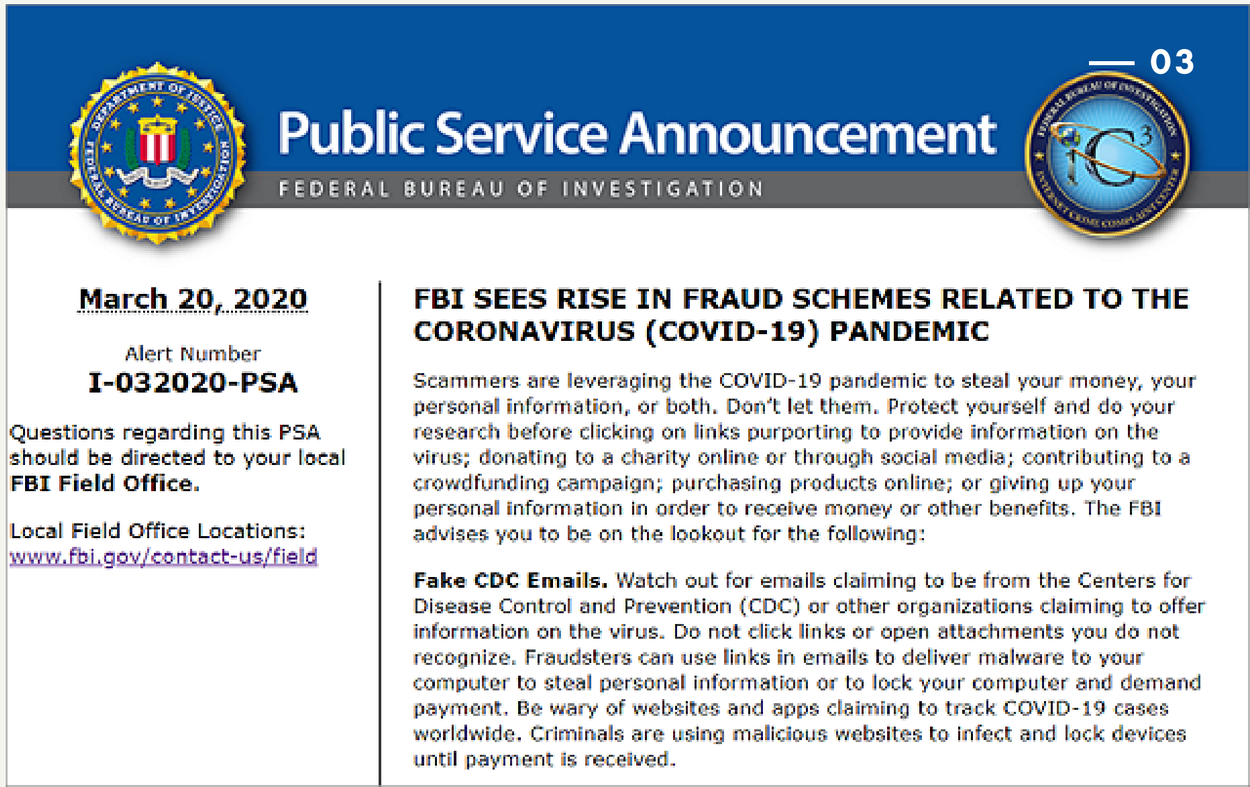
垃圾郵件

電子郵件是最適合做社交工程攻擊的工具

- 可偽裝寄件者
- 低成本且可大量發送
- 容易使用，無技術門檻
- 可輕易利用被害者協助攻擊他人的電子郵件，
  ex：轉寄電子郵件給親友、同事

最喜歡利用最熱門的新聞時事發動攻擊

2020年3月，美國聯邦調查局(FBI) 發布的新聞稿：以新冠病毒（COVID-19）為主題的詐騙攻擊正持續地增加。網路罪犯利用新冠病毒全球大流行之事件，對企業及政府發動社交工程攻擊。



如何防範電子郵件社交工程

不開啟來路不明的電子郵件及附加檔案

1. 檢查**寄件者名稱**與**信箱**
2. 以郵件**主旨**評估是否有必要開啟郵件
3. 檢查郵件內的**連結**是否正確
4. 檢查郵件附檔的**副檔名**，是否為常見可含有病毒的檔案名稱，ex：*.bat、*.pif、*.exe、*.zip、*.src、*.cmd、*.rar等
5. 轉寄郵件時刪除寄件者與收件者資料，並使用密件傳送

教育部社交工程演練

資通安全事件通報及應變辦法 §8：每半年辦理一次社交工程演練。

- 社交工程為駭客常用入侵管道，透過電子郵件夾帶惡意程式或連結網址等方式，輔以吸引人之信件主旨及內容，誘使缺乏警戒心的使用者開啟後造成進一步破壞，嚴重損害機關或個人之權益。
- 演練方式為模擬駭客寄送各種誘騙的測試信件給本校同仁，測試受測者之資安意識。
- 透過實施演練，提升教育體系人員針對社交工程攻擊之警覺性，降低社交工程風險。
- 參與演練人員為學校全體人員（具備公務電子郵件帳號者），不限於正式公務人員。
- 依據本校資訊安全推行委員會第十八次會議決議，「違反社交工程」之教職員生，將強制選讀相關資訊安全課程。

教育部社交工程演練

110年演練期間：5月～11月間進行2次

- 依規定提交之演練人員名單， 按人員類型隨機選取 100人，**主管人員（組長）以上原則佔受測人員總數35%以上**。

1. 不預覽信件
2. 純文字讀取
3. 封鎖圖片

檢查網址

檢查副檔名

不能「開啟/預覽」郵件？

您可能覺得只要不開郵件附件和不點擊連結，就不會中招...

- 但有些惡意程式是利用ActiveX功能來執行的，而HTML可以撰寫ActiveX。
- 若您的電子郵件是HTML格式，只要瀏覽電子郵件，就會觸發裡面的ActiveX執行，連結到惡意程式網站下載病毒程式。

Q：看不見郵件內容，如何判斷是否為社交工程郵件？

A：以「純文字格式讀取」瀏覽內容取代HTML格式

教育部社交工程演練-實際案例（以不同模式讀取信件）

一般開啟

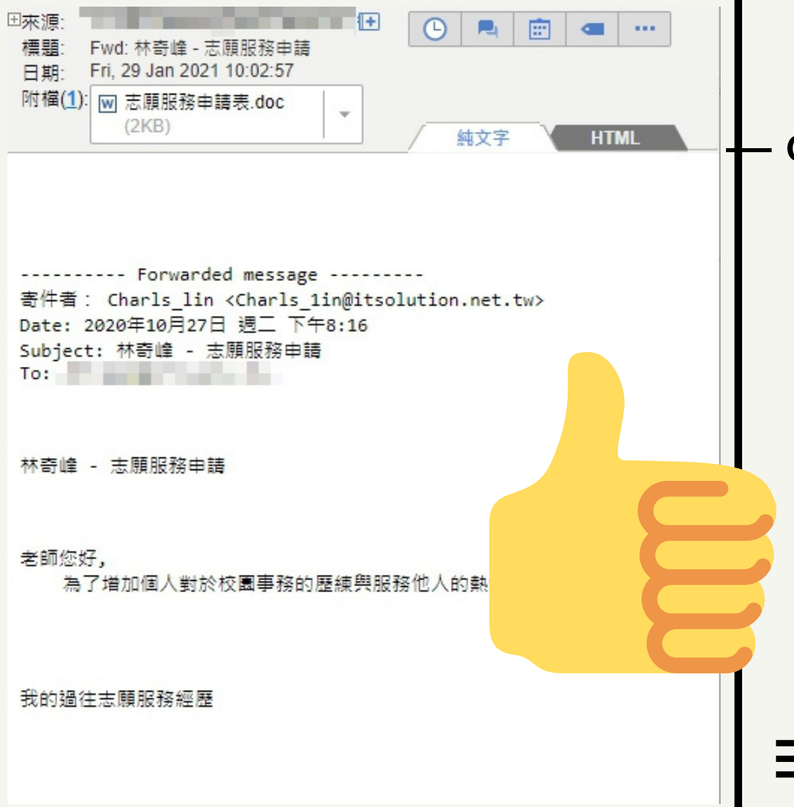
開啟的信件後自動下載圖片，並執行圖片中夾帶的程式

關閉「自動下載圖片」

使用者確認信件內容沒問題後，才解除封鎖，下載圖片

純文字讀取

信件內容不攜帶任何格式，是最安全的讀取方式；確認信件內容沒問題後，可切換html(一般)格式讀取完整內容



校園真實攻擊案例

案例１－偽造的信件及釣魚網頁

尊敬的電子郵件帳戶用戶，

您的郵箱已超出電子郵件幫助設置所設置的存儲空間限制，您必須重新驗證以接收新郵件。

單擊此 https://taiwan3232424.cabanova.com/index.html

注意：如果您不回复此電子郵件，我們的數據庫將禁用您的帳戶，並且您將不再接收或發送電子郵
件。

很抱歉給您帶來不便。

版權 2021
台灣電子郵件網絡郵件服務台
版權所有

From:系統管理者< @nccu.edu.tw>
Date: Thu, 23 Sep 2021 06:50:31
Subject: 重要通知

親愛的用戶

我們注意到您的郵箱出現了一些未經授權的登錄嘗試。 因此，我們建議您立即驗證您的帳戶。 請單擊下面的鏈接並使用您的詳細信息登錄，以避免您的帳戶被禁用。
感謝您幫助我們保護您。 點擊這裡>> <https://virl.ws/s/nccu-edu-tw/>

NCCU 管理團隊
© 2021 國立政治大學。 版權所有。

- 雖已檢查寄件者為校內信箱，但實際上該信箱已遭駭客登入。
- 應**檢查連結網址**是否正確！

本校Email網址 https://nccu.edu.tw/indexs.html

案例２－收到寄件者顯示自己信箱的恐嚇信

- 可透過mail2000信箱查看最近的**IP登入紀錄**
- 有無異常的IP登入紀錄
  - 有：表示確實遭駭客入侵，應**立即更換email密碼**
  - 無：表示對方冒用您的email名義寄出（在電子郵件機制中，寄件者是可以修改自己的寄件人顯示名稱/帳號的）

常見

- 長期對策：
  - 基本MailGates(郵件過濾系統)會過濾此種異常信件，**勿將自己的信箱設定為白名單**，就不會收到學校以外的信件以自己帳號名義寄信過來了。
  - 因為MailGates系統只會過濾校外email主機寄來的郵件，透過學校信箱寄信給自己仍是可以收到的!

電子郵件信箱安全性設定

安全性設定/校園電子郵件信箱Mail2000

1. 關閉信件預覽功能
2. 純文字讀取
3. 封鎖圖片/關閉自動下載圖片功能

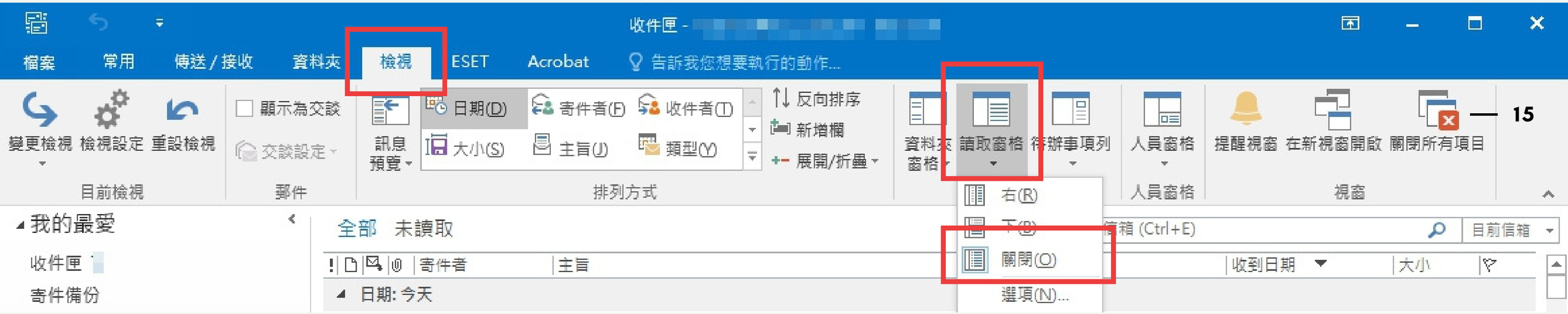
安全性設定/教育版Gmail信箱 G Suite (g.nccu.edu.tw)

1. 關閉信件預覽功能

2. 封鎖圖片/關閉自動下載圖片功能

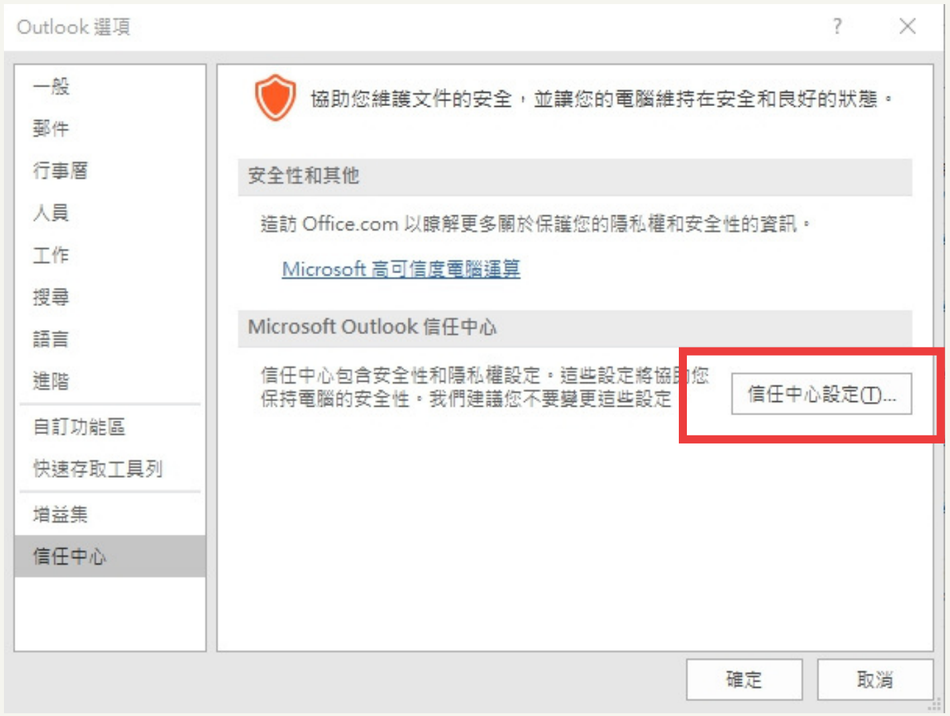
安全性設定/Microsoft Outlook信箱 (2010、2013、2016)

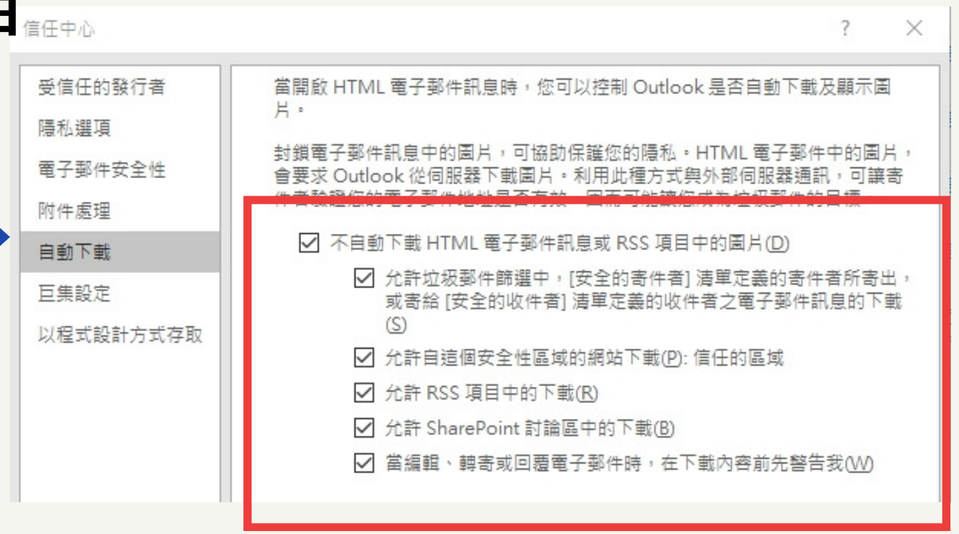
1. 關閉信件預覽功能



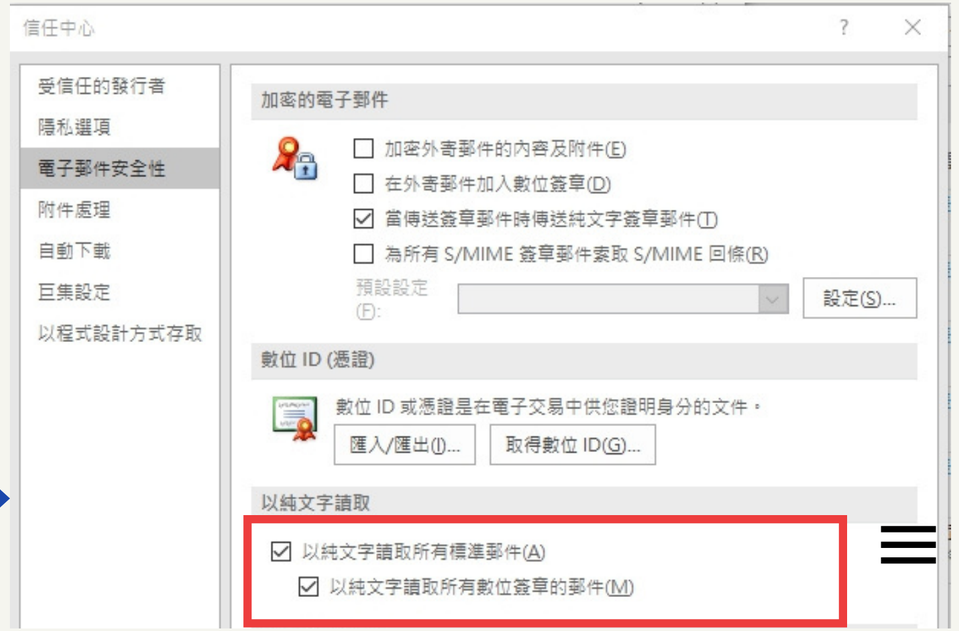
安全性設定/Microsoft Outlook信箱

2. 封鎖圖片/關閉自動下載圖片功能





3. 純文字讀取



安全性設定/ 行動裝置郵件信箱

iPhone郵件信箱

1. 關閉信件預覽功能

在收件匣列表中，「郵件」預設為顯示每封電子郵件的兩行文字

前往「設定」 >「郵件」>「預覽」，然後選擇「無」

2.不自動下載圖片

「設定」 >「郵件」> 取消選擇「載入遠端影像」

Android郵件信箱

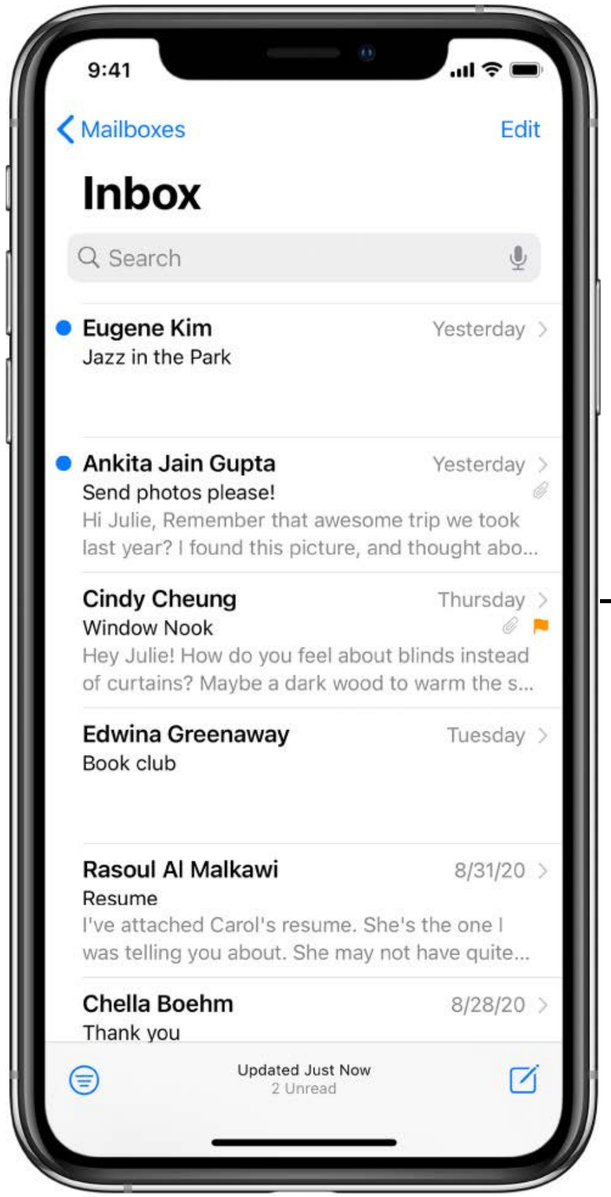
1. 關閉信件預覽功能

「設定」 >「顯示」>「無」

Gmail APP

1. 不自動下載圖片

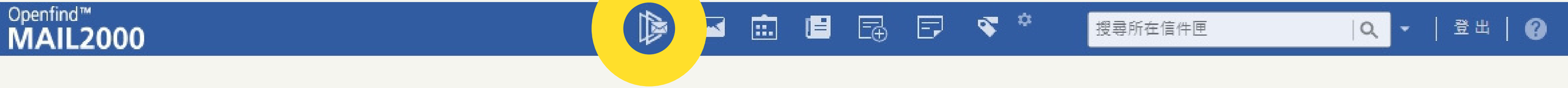
「三」>「設定」 >「數據用量」下方「圖片」>「顯示不明外部圖片時，必須先詢問我」



更進一步的防護設定

MailGates 雙重認證 @Mail2000 APP

電子郵件防護系統 MailGates



NCCU MailGates 郵件防護系統

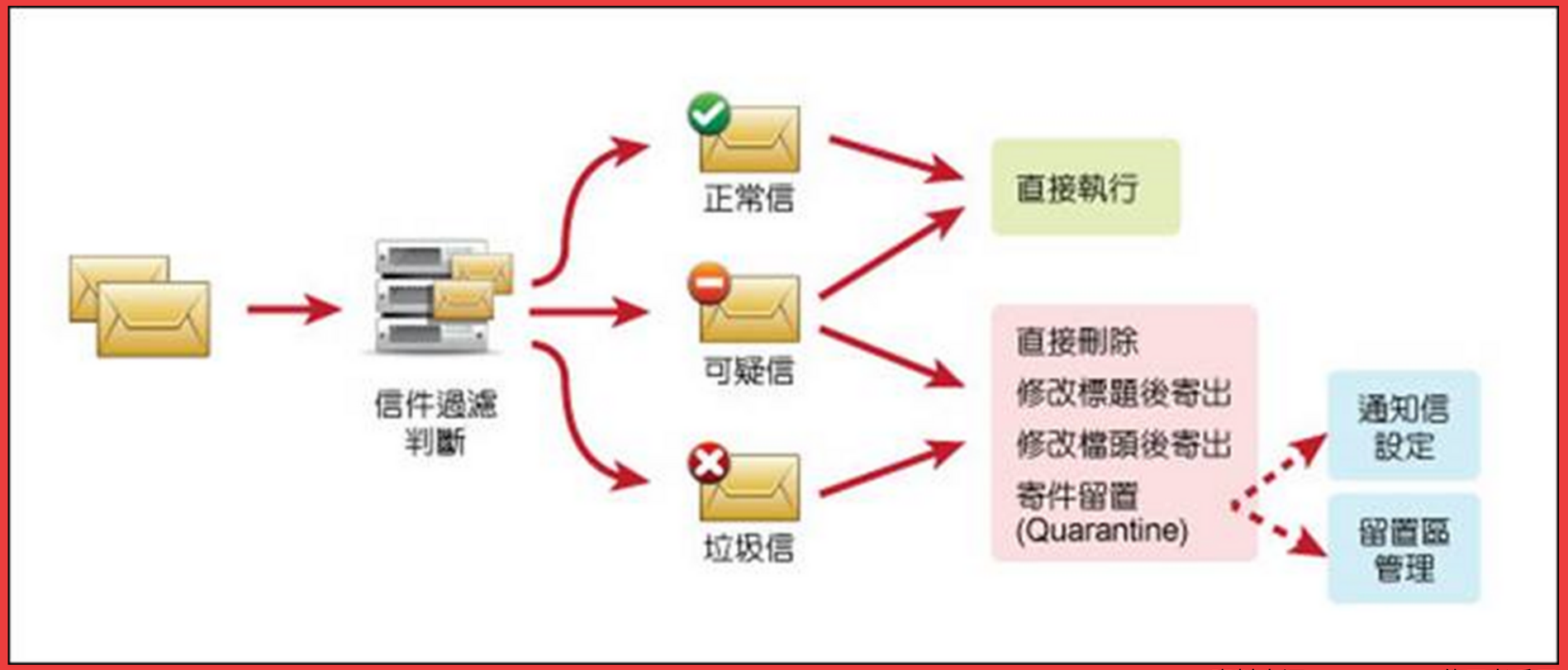
NCCU 電子郵件伺服器

個人 電子郵件收件夾

部署於本校電子郵件伺服器前端之 MailGates 郵件防護系統，透過分析自動偵測並過濾各式垃圾郵件

可疑信？

當 MailGates 依據過濾規則無法判斷一封信為正常信或垃圾信時，
可依據使用者設定的處理原則，將信件直接刪除、做修改後繼續送至信箱，
或是將其留置在 MailGates 主機上。



資料來源：MailGates 使用者手冊

把可疑信加上TAG設定

可疑信仍送至信箱，避免誤攔
但於主旨加上TAG，提醒收件者

雙重認證/登入 Mail2000 加強版安全機制

使用雙重驗證機制必須先在行動裝置安裝 @Mail2000 APP。
當使用帳號密碼登入後，系統會推播一組認證碼到註冊的手持裝置上，輸入該組認證碼方可登入。

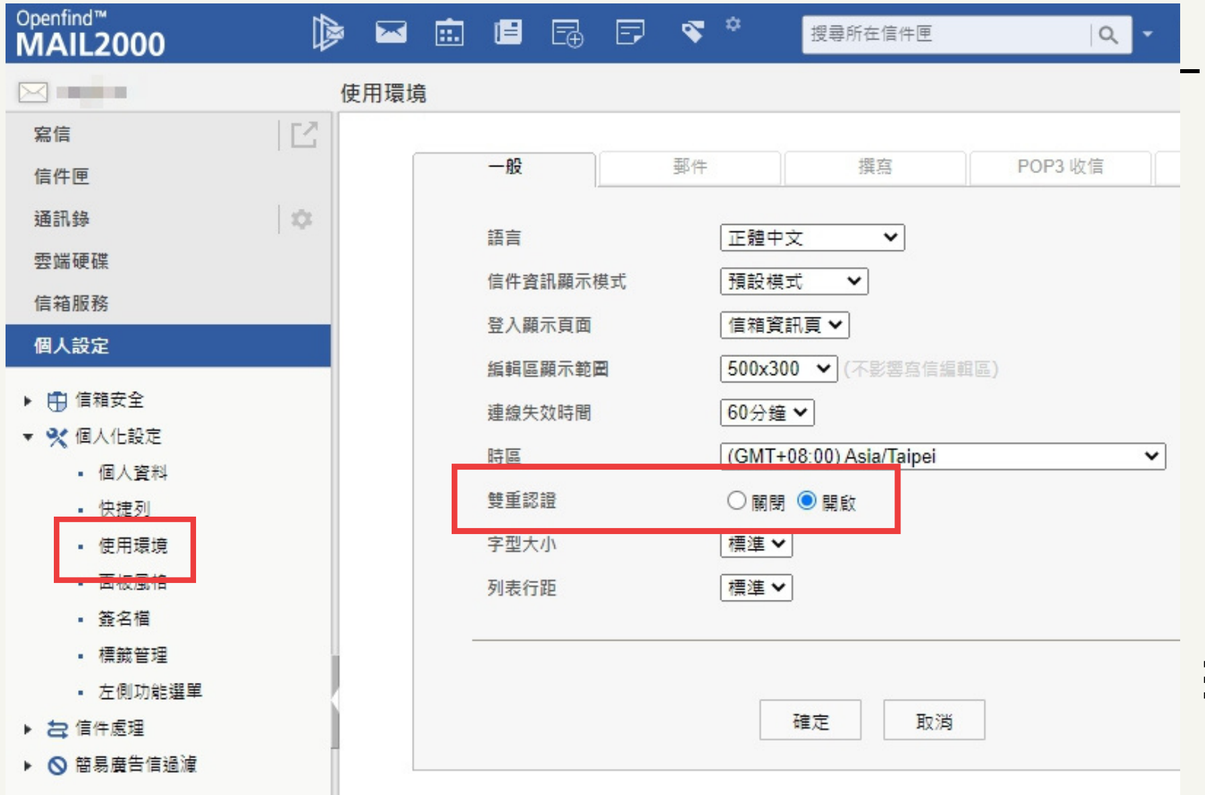
- 行動裝置

1. 透過 Google Play 下載並安裝 @Mail2000 APP

2.@Mail2000設定

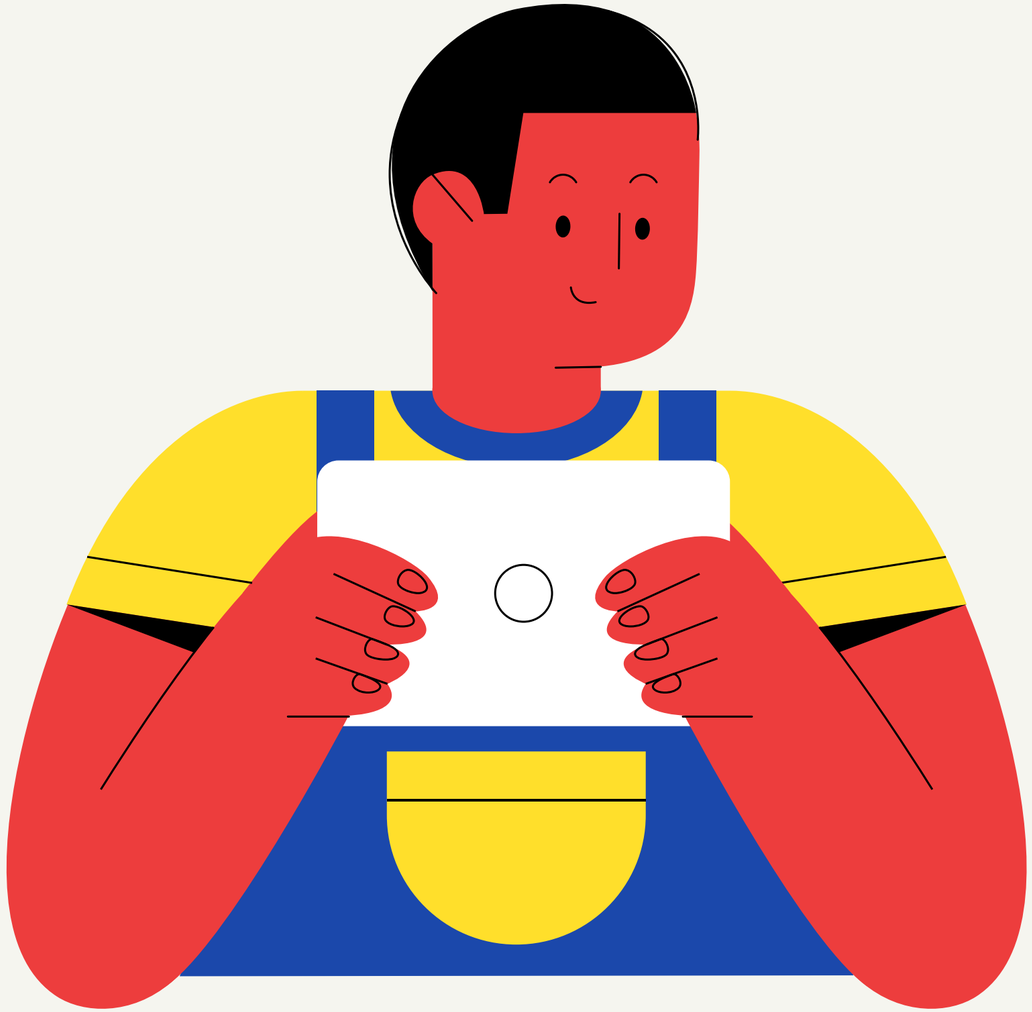
- Web mail

「個人設定」>「使用環境」> 勾選「雙重驗證」



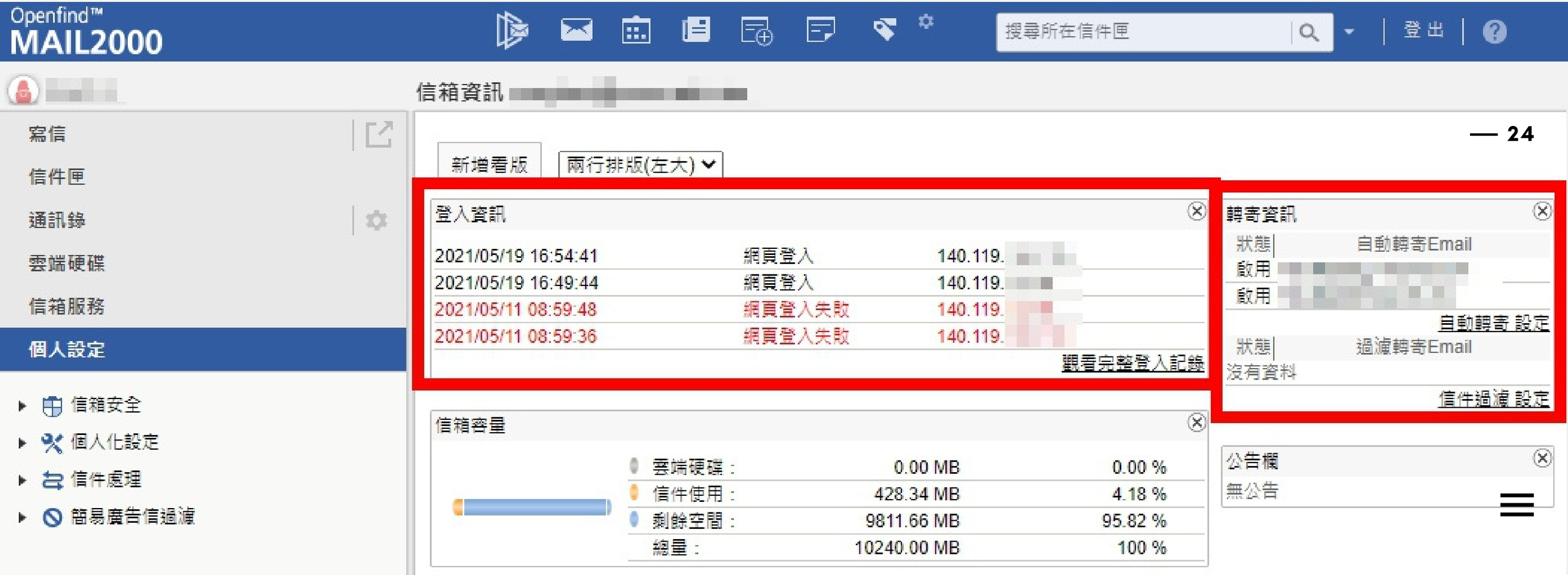
平常的警覺性

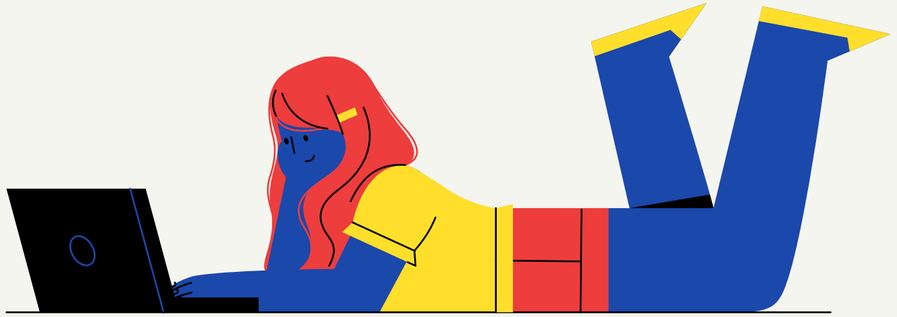
登入IP紀錄
轉寄設定



習慣性查看登入IP紀錄、信箱轉寄設定

1. 平常登入時看一眼登入紀錄，留意有無異常IP的登入紀錄。(系統最多記錄登入成功及失敗各100筆資訊)
2. 有遭駭客成功登入過的使用者，務必確認有無被設定自動轉寄信件至其他外部信箱。





Thanks for Watching.