新任資訊組長基礎知能培訓研習
電腦端點防護與全市防毒授權軟體安裝

教資科資安組 林延昌 2024.08.16

#法規

- **刑法第315-1條**
  - 有下列行為之一者，處三年以下有期徒刑、拘役或三十萬元以下罰金：
  - 一、無故利用工具或設備窺視、竊聽他人非公開之活動、言論、談話或身體隱私部位者。
  - 二、無故以錄音、照相、錄影或電磁紀錄竊錄他人非公開之活動、言論、談話或身體隱私部位者。
- **刑法第358條**
  - 無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金。
- **刑法第359條**
  - 無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科六十萬元以下罰金。
- **刑法第360條**
  - 無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金。

資安組關心您

#本日課程大綱

- **技術控制措施**
  - 特洛伊木馬病毒演示
  - 駭入WordPress架站演示
  - 駭入Win7演示
  - 駭入NAS演示
  - 強化校園資安聯防
- **人員控制措施**
  - 提升資安素養
  - 防範社交工程
- **實體控制措施**
  - 繞過密碼方法
- **組織控制措施**
  - 強化資通安全管理

資安組關心您

#技術

- 特洛伊木馬病毒演示
- 駭入WordPress架站演示
- 駭入Win7演示
- 駭入NAS演示

資安組關心您

#技術-駭客駭入電腦第一件事

- Set-MpPreference -DisableRealtimeMonitoring $true

資安組關心您

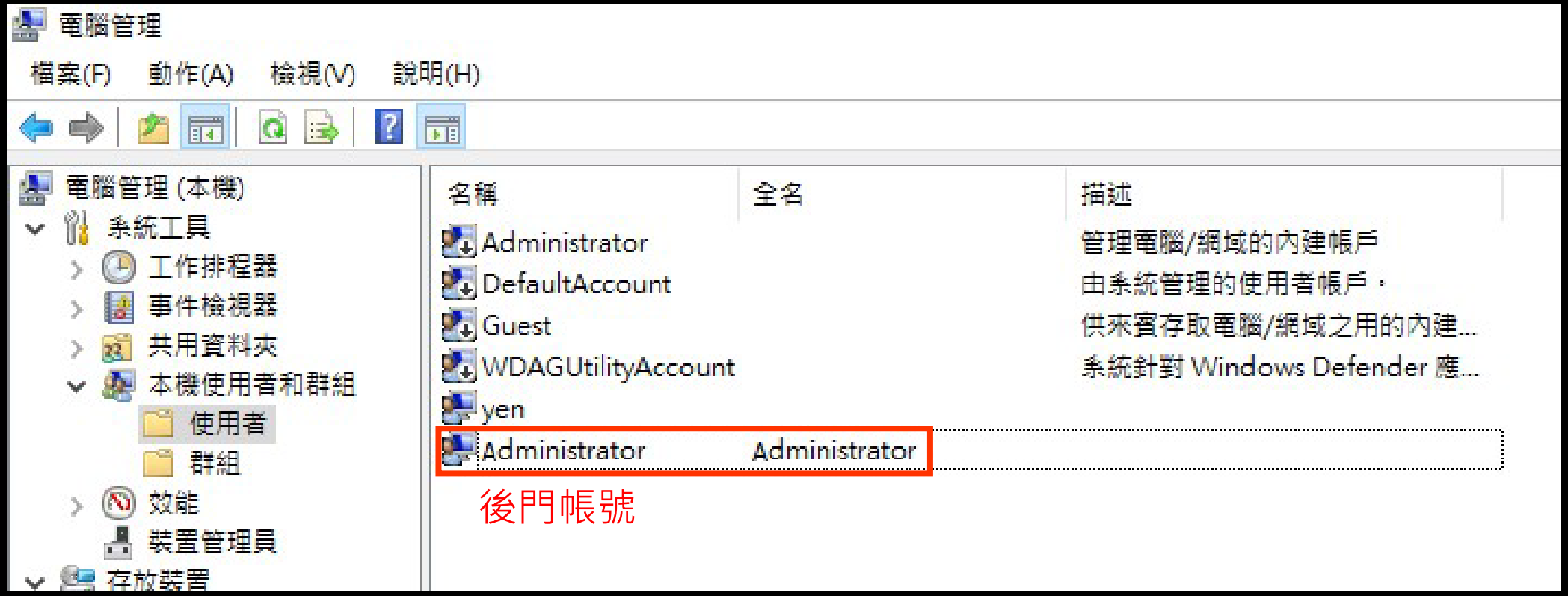
#技術-防毒軟體正常啟用狀態

- 搜尋「病毒與威脅防護」>病毒與威脅防護設定「管理設定」

資安組關心您

#技術-帳號清查

- WIN開始圖示滑鼠右鍵「電腦管理」>「本機使用者和群組」>「使用者」



資安組關心您

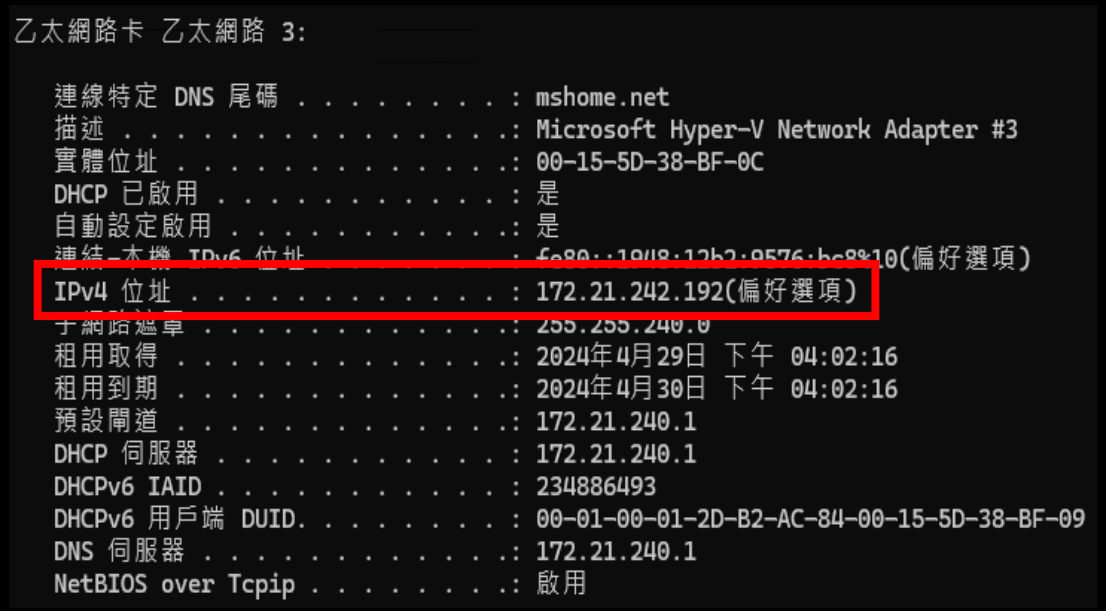
#技術-安裝集中式防毒並執行掃描

- https://mis.ntpc.edu.tw/p/412-1001-1101.php

資安組關心您

#技術-查詢自己IP位置

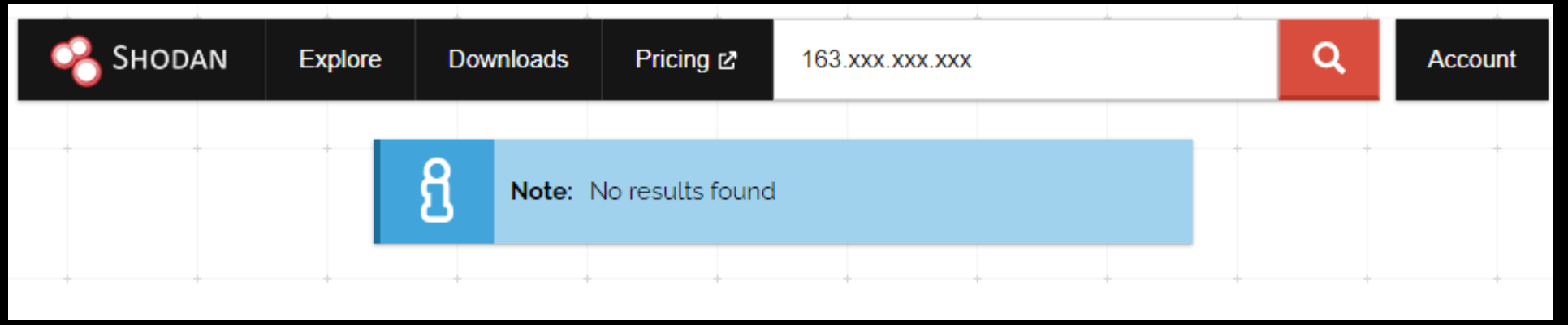
- 按下Windows + R 開啟「執行」視窗後，輸入「cmd」後點選選確定 。
- 輸入「ipconfig /all」送出，在 IPv4 位址後面就是此台電腦的IP。
- 行政電腦應為虛擬IP(IP第一碼是10或172或192)。



資安組關心您

#技術- Shodan查詢

- https://www.shodan.io/
- 在搜尋欄輸入實體IP位置
- 結果應為Note:No results found



資安組關心您

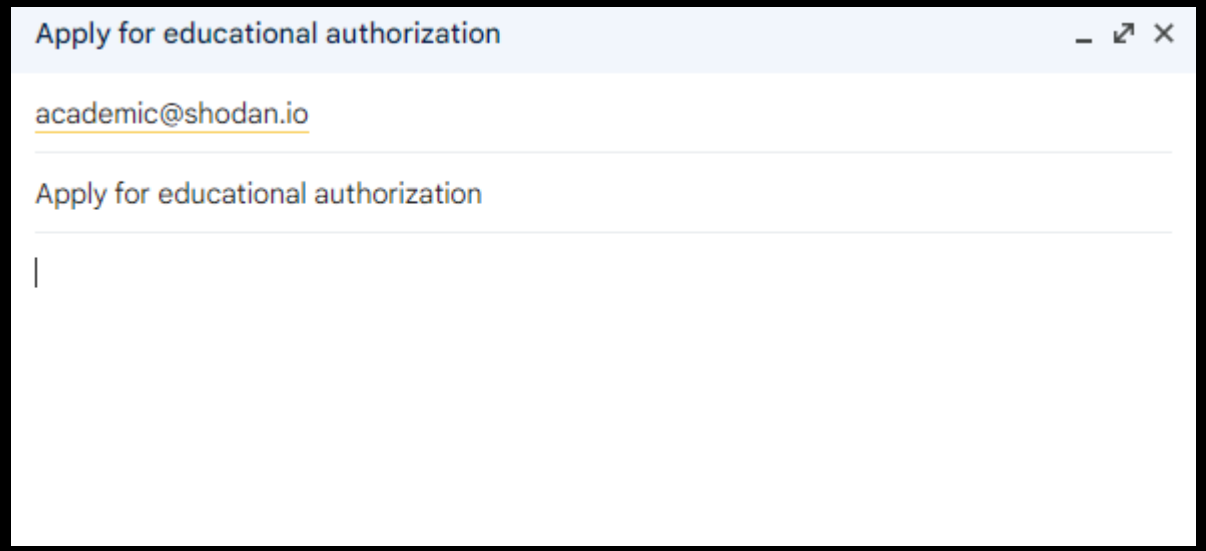
#技術- Shodan網段查詢

- https://mis.ntpc.edu.tw/p/412-1001-78.php?Lang=zh-tw
- 點選「連線單位IPv4分配」>輸入校務行政系統帳密>開始下載
- Excel表格欄位「LAN1 IP / SM」，即為貴校「實體IP網段」
- Shodan使用網段查詢，需要登入，可連結google教育帳號(@apps.ntpc.edu.tw)
- 在Shodan搜尋欄輸入「net:xxx.xxx.xxx.xxx/xx」

資安組關心您

#技術- shodan教育權限申請

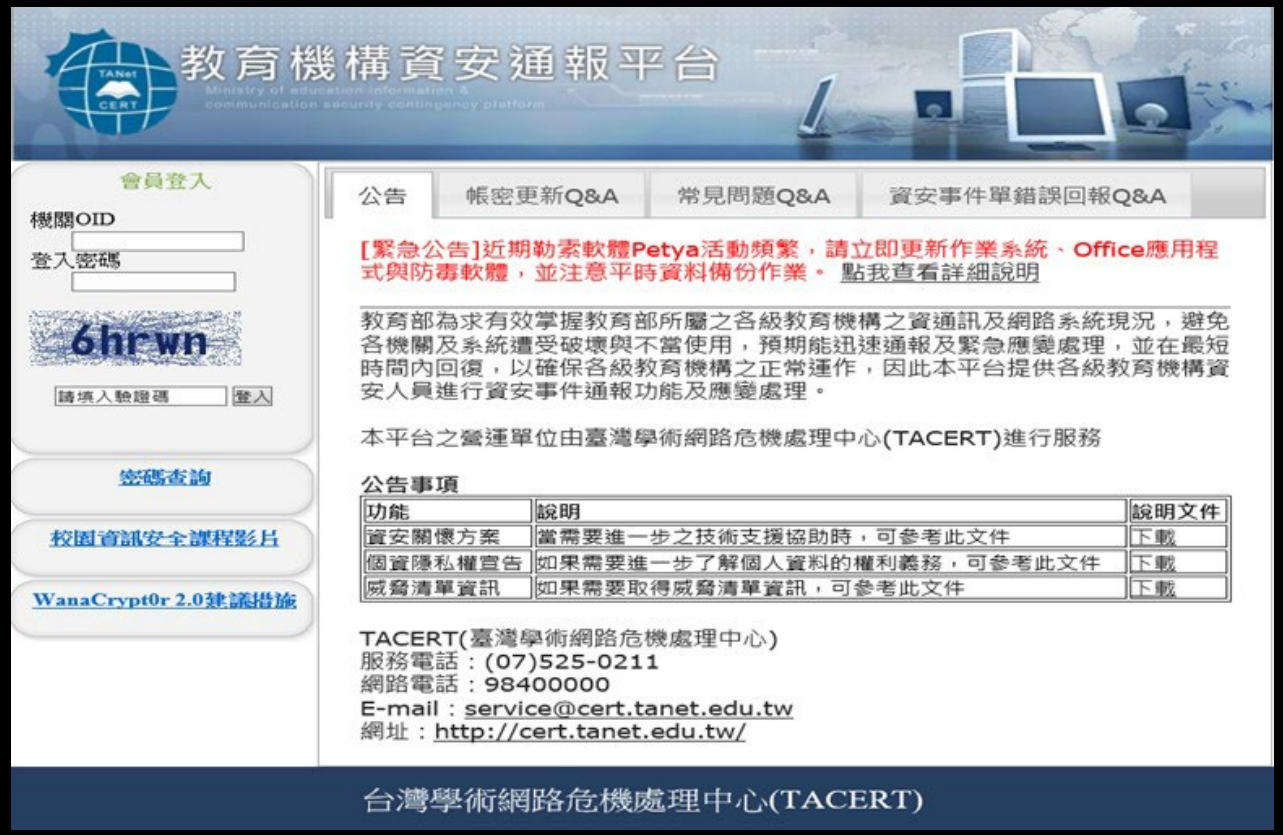
- 用google教育帳號(@apps.ntpc.edu.tw)寄信至如下：
  - 收件者：academic@shodan.io
  - 主旨：Apply for educational authorization
  - 內容：可空白
  - 差異：可看到更多頁結果



資安組關心您

#技術-教育機構資安通報平台(1/4)

- https://info.cert.tanet.edu.tw/prog/index.php

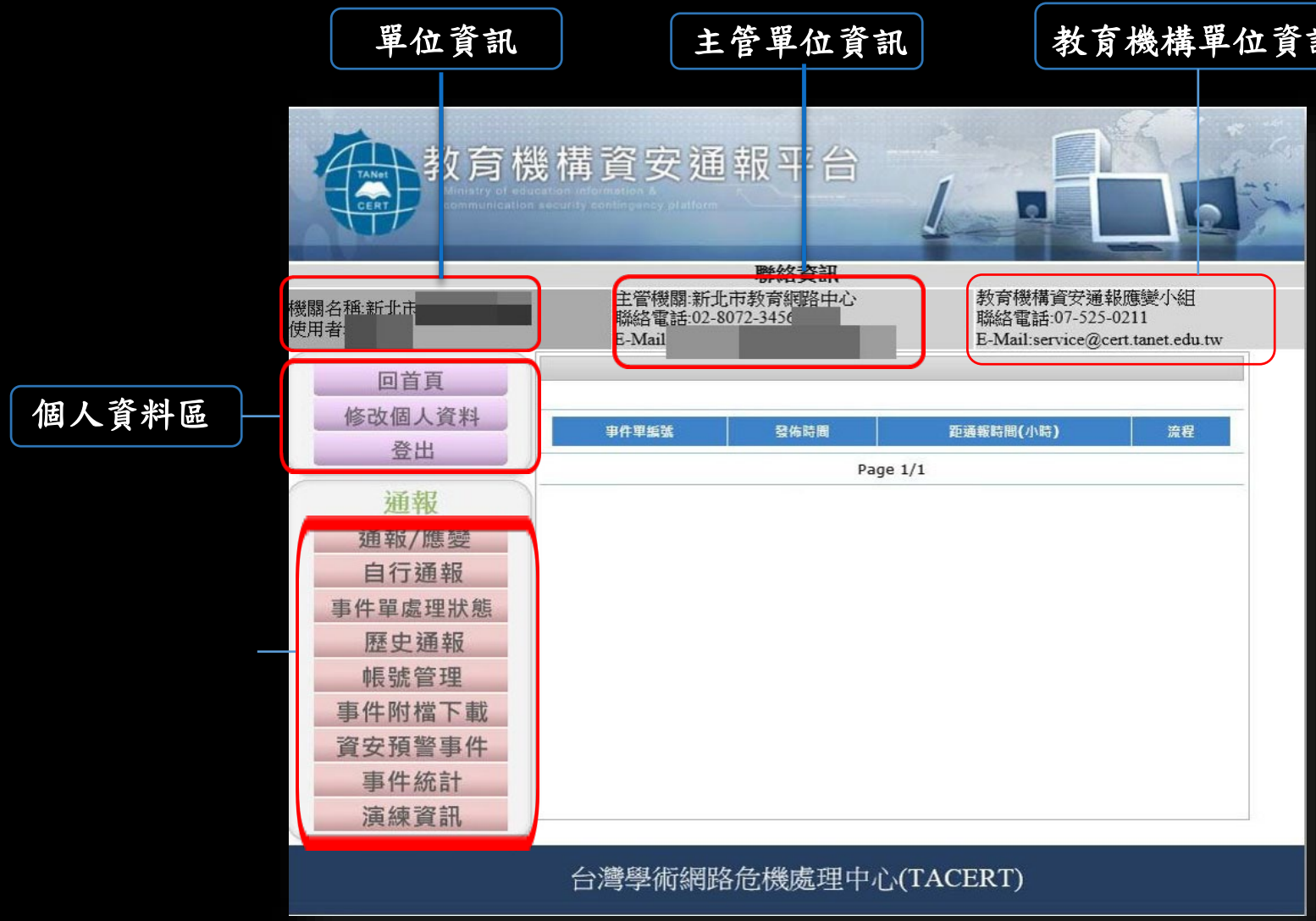


- 會員登入
  - 使用OID帳號登入
  - 一個學校至少兩位聯絡人
  - 每個聯絡人OID密碼可不同

- 忘記密碼
  - 點選密碼查詢
  - 詢問前校內資安通報承辦人
  - 聯絡TACERT(臺灣學術網路危機處理中心)
    服務電話：(07)525-0211

資安組關心您

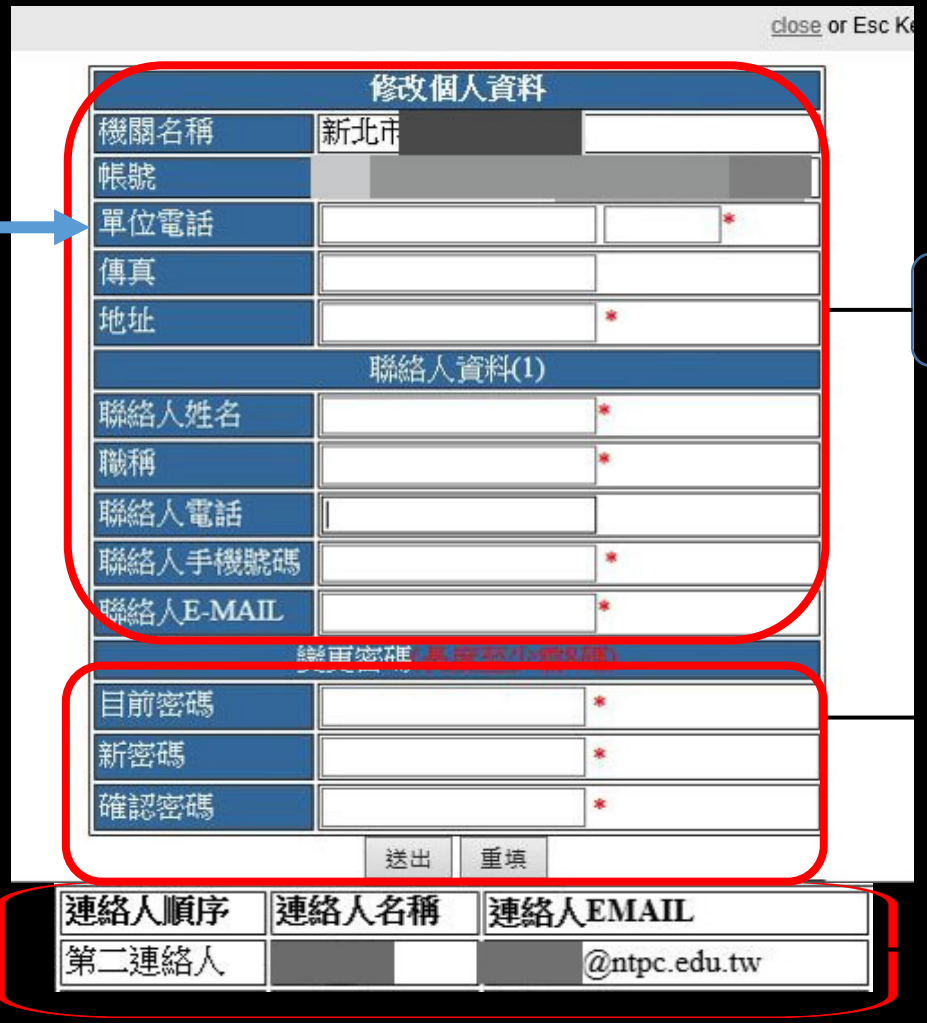
#技術-教育機構資安通報平台(2/4)



資安組關心您

#技術-教育機構資安通報平台(3/4)

- 第二聯絡人很常修改到機關單位電話，導致第一聯絡人電話與電二聯絡人相同。



資安組關心您

#技術-教育機構資安通報平台(4/4)

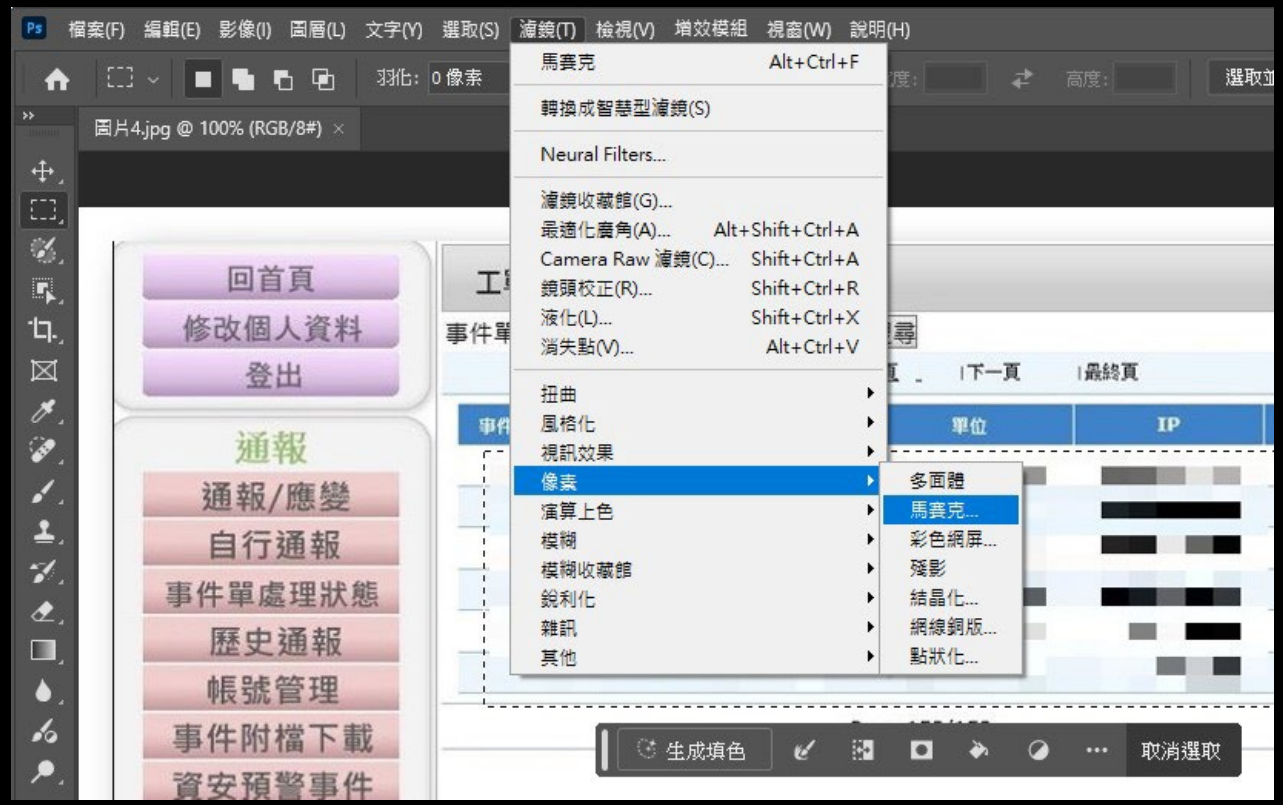
Log紀錄：

- 結束時間
- 來源位置
- 來源連接埠
- 目標位置
- 目標連接埠

資安組關心您

#技術-遮罩

- https://mis.ntpc.edu.tw/p/404-1001-9049.php



資安組關心您

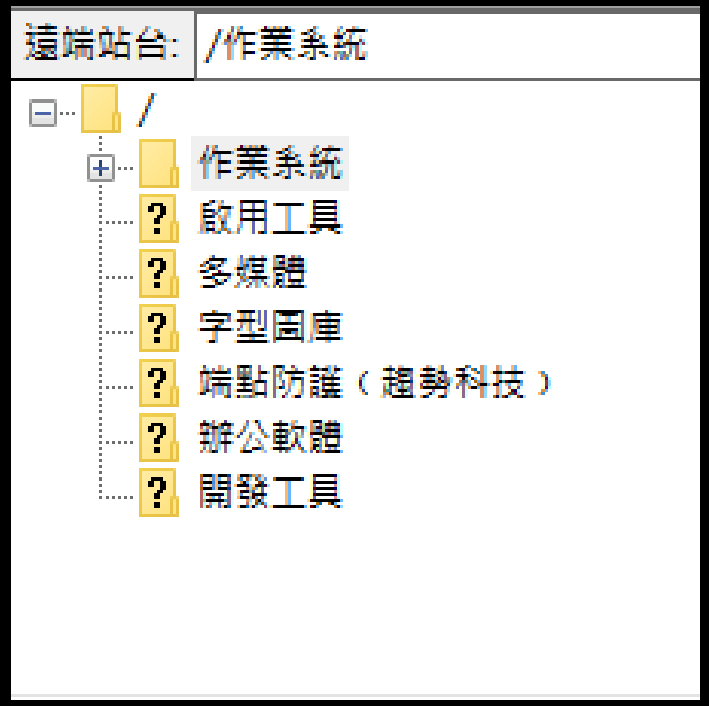
#技術-VPN

- https://bdp.ntpc.edu.tw/

資安組關心您

#技術-FTP

- ftp://ftp.ntpc.edu.tw/



資安組關心您

#技術-法遵事項

- **資通安全責任等級分級辦法第7條**
  - 各機關自行辦理資通業務，未維運自行或委外設置、開發之資通系統者，其資通安全責任等級為 D 級。
- **資通安全責任等級分級辦法第6條**
  - 各機關維運自行或委外設置、開發之資通系統者，其資通安全責任等級為 C 級。
  - 前項所定自行或委外設置之資通系統，指具權限區分及管理功能之資通系統。

#技術-資安是攻防拉鋸戰

CVE-2024-0518	Type confusion in V8 in Google Chrome prior to 120.0.6099.224 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2024-0517	Out of bounds write in V8 in Google Chrome prior to 120.0.6099.224 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2024-0333	Insufficient data validation in Extensions in Google Chrome prior to 120.0.6099.216 allowed an attacker in a privileged network position to install a malicious extension via a crafted HTML page. (Chromium security severity: High)
CVE-2024-0225	Use after free in WebGPU in Google Chrome prior to 120.0.6099.199 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2024-0224	Use after free in WebAudio in Google Chrome prior to 120.0.6099.199 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2024-0223	Heap buffer overflow in ANGLE in Google Chrome prior to 120.0.6099.199 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2024-0222	Use after free in ANGLE in Google Chrome prior to 120.0.6099.199 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-7024	Heap buffer overflow in WebRTC in Google Chrome prior to 120.0.6099.129 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-6707	Use after free in CSS in Google Chrome prior to 120.0.6099.109 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2023-6706	Use after free in FedCM in Google Chrome prior to 120.0.6099.109 allowed a remote attacker who convinced a user to engage in specific UI interaction to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-6705	Use after free in WebRTC in Google Chrome prior to 120.0.6099.109 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-6704	Use after free in libavif in Google Chrome prior to 120.0.6099.109 allowed a remote attacker to potentially exploit heap corruption via a crafted image file. (Chromium security severity: High)
CVE-2023-6703	Use after free in Blink in Google Chrome prior to 120.0.6099.109 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
CVE-2023-6702	Type confusion in V8 in Google Chrome prior to 120.0.6099.109 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)

- Google Chrome 瀏覽器在 2023 年發現359個漏洞
- 短時間內高風險漏洞
- 零時差漏洞 (Zero-Day Vulnerability)
- 進階持續性滲透攻擊（Advanced Persistent Threat, APT）
- 防火牆被繞過後？

資安組關心您

#人員-駭客？(1/4)

資安組關心您

#人員-駭客？(2/4)

- 駭客開發的工具、腳本與軟體。
- 非凡技術、惡意、破壞。
- 自殺型駭客。
- 網路恐怖主義。
- 國家級駭客。

ex:伊朗核電廠 stuxnet

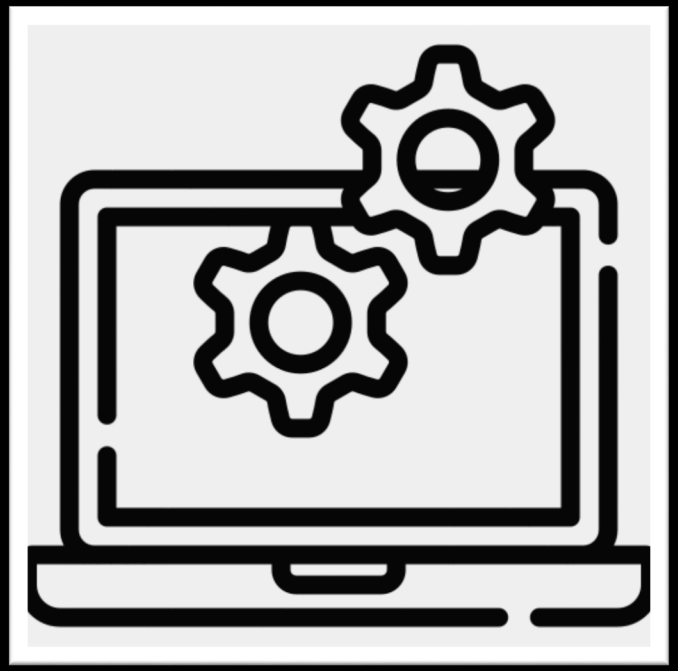
資安組關心您

#人員-駭客？(3/4)

- 經「授權」
  才是「白帽駭客」。

資安組關心您

#人員-駭客？(4/4)



技術

興趣

特質

資安組關心您

#人員-提升資安素養

- **新北市教育資料平台**
  - https://bdp.ntpc.edu.tw/
- **新北星聯盟(數位星球)**
  - 親師生平台>新北市專區>新北星聯盟(數位星球)
  - https://pts.ntpc.edu.tw/
- **數位學習影音網**
  - 親師生平台>新北市專區>數位學習影音網>課程總覽>資訊安全
  - https://pts.ntpc.edu.tw/
- **edu磨課師+**
  - 親師生平台>教育部專區>磨課師平台>依類別>資訊工程>資訊安全
  - https://pts.ntpc.edu.tw/

資安組關心您

#人員-提升資安素養

資安組關心您

#人員-提升資安素養

資安組關心您

#人員-提升資安素養

資安組關心您

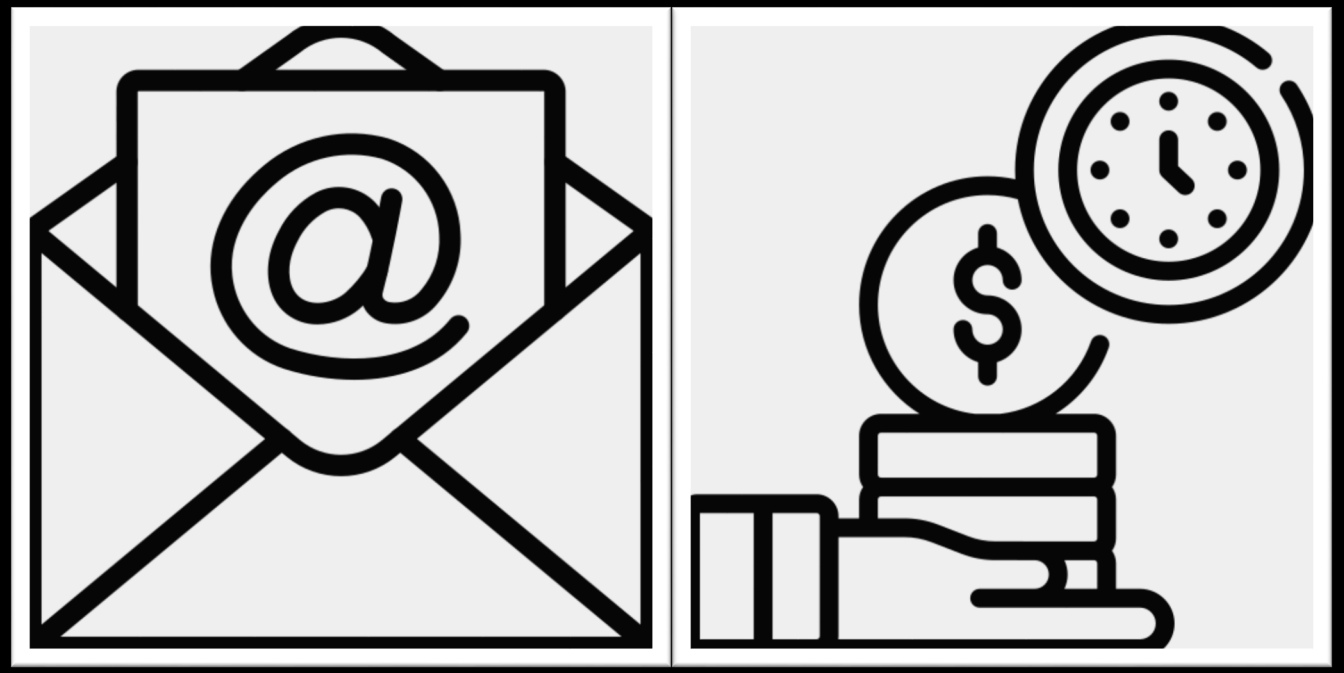
#人員-提升資安素養

資安組關心您


網路使用要注意
資通安全沒煩惱
ID:XXXX
Passord:XXXX
新北星聯盟
新北市政府 教育局
新北智慧學習

#人員-社交工程

VS



滲透

社交工程

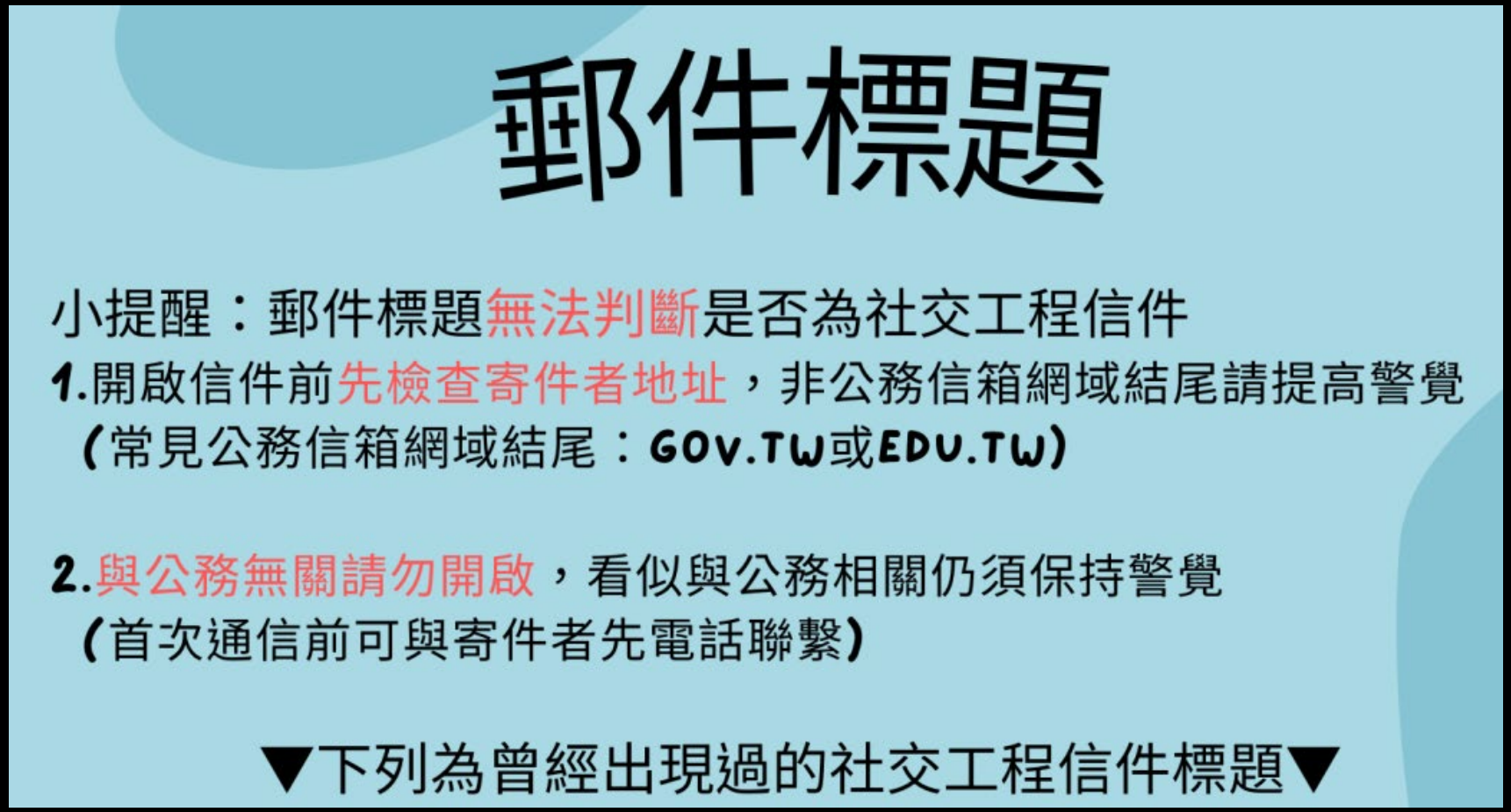
資安組關心您

#人員-防範社交工程測驗

- Jigsaw | 網路詐騙知多少(共8題)
- https://phishingquiz.withgoogle.com/?hl=zh-TW

資安組關心您

#人員-郵件標題無法判斷(1/2)



資安組關心您

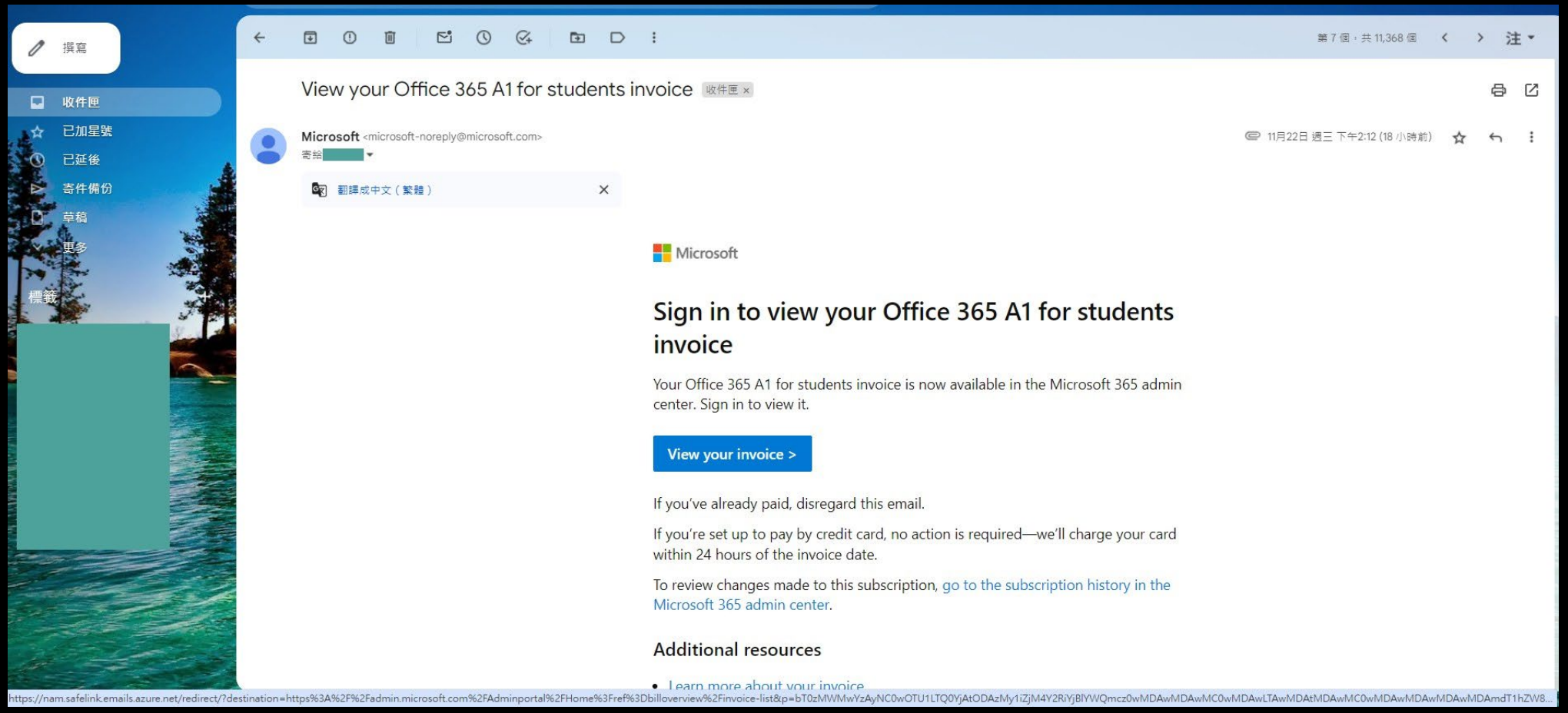
#人員-郵件標題無法判斷(2/2)

資安組關心您

#人員-實際釣魚郵件案例(1/2)

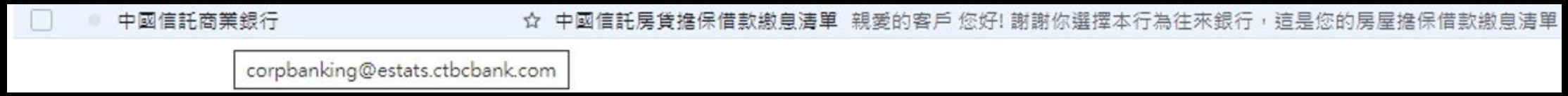
資安組關心您

#人員-實際釣魚郵件案例(2/2)



資安組關心您

#人員-非社交工程電子郵件案例(1/2)

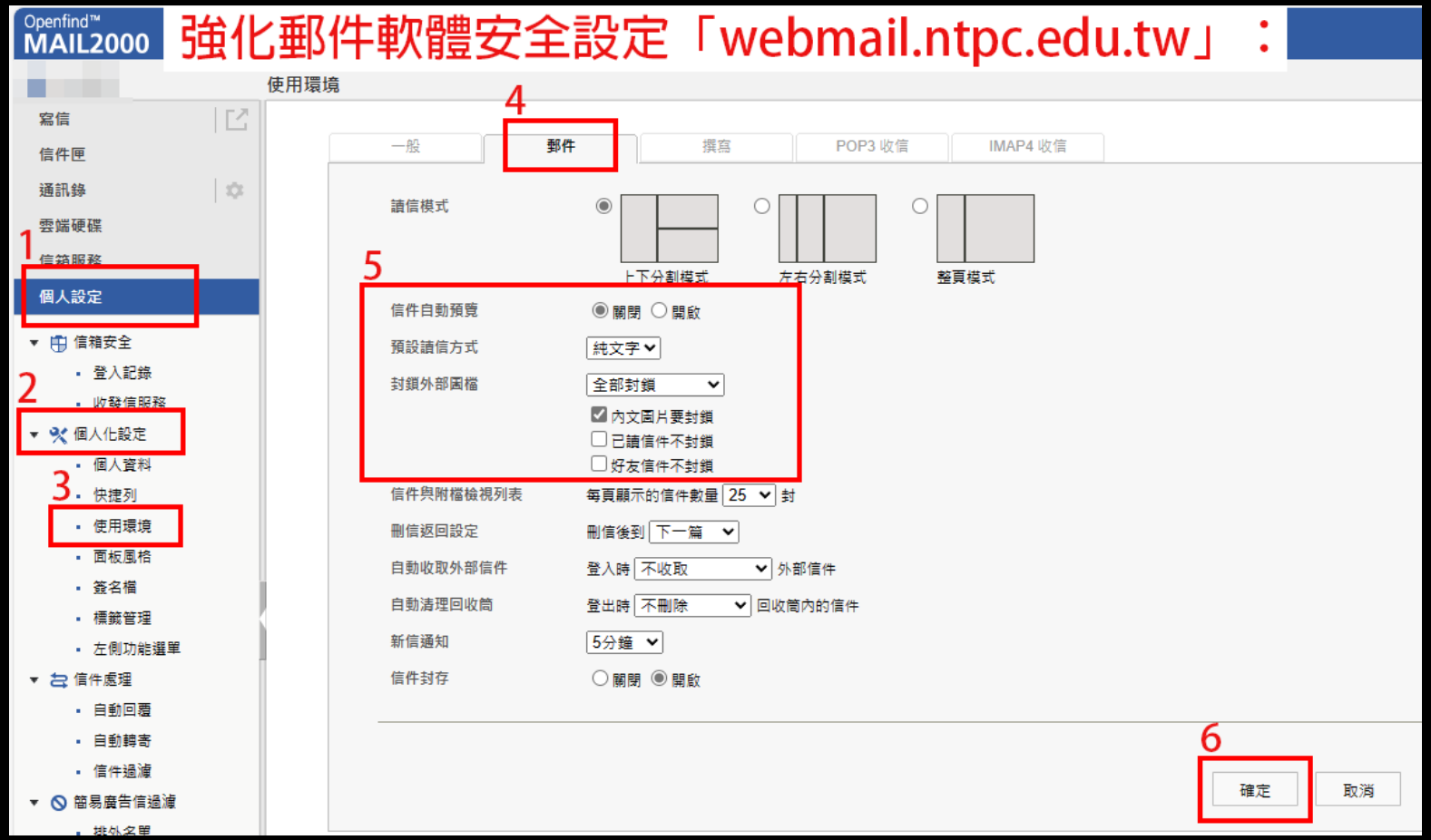


資安組關心您

#人員-非社交工程電子郵件案例(2/2)

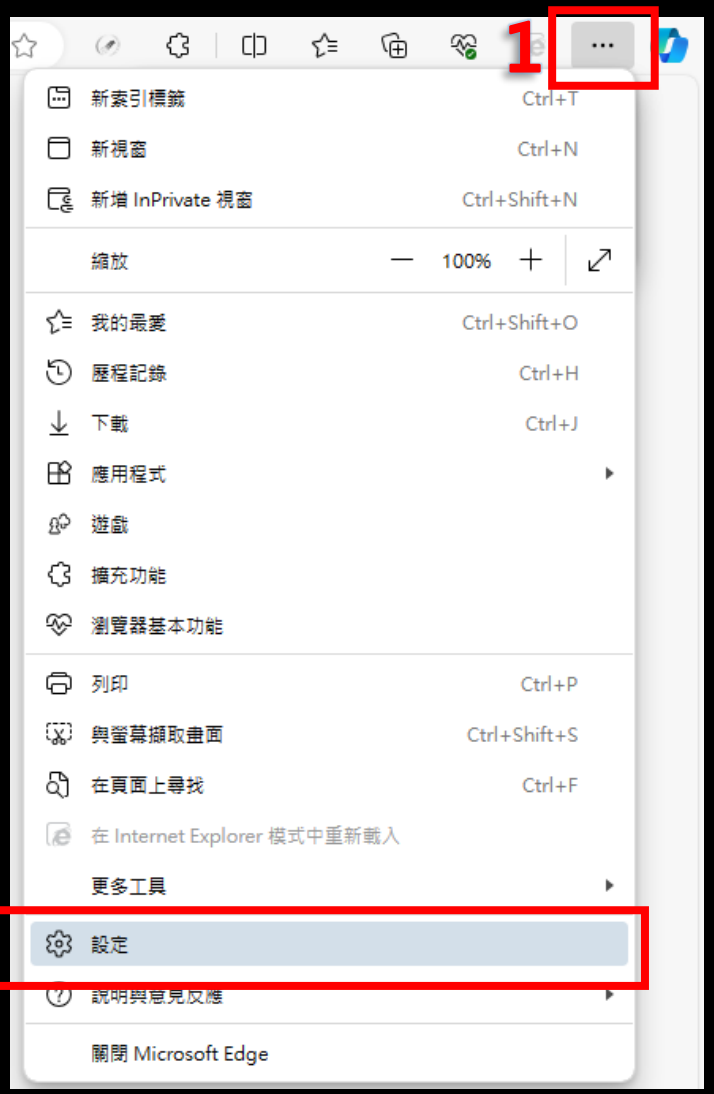
資安組關心您

#人員-防範社交工程郵件_純文字模式



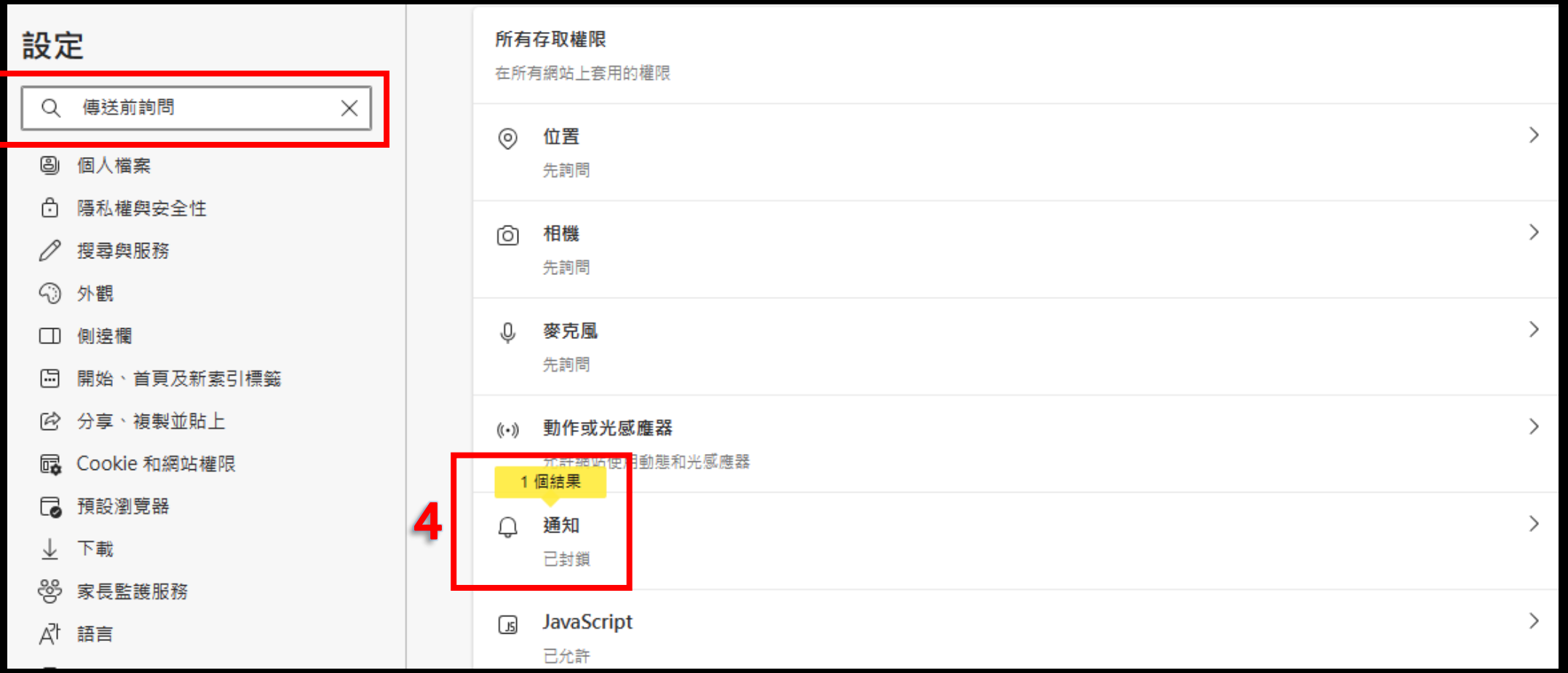
資安組關心您

#人員-Edge封鎖通知(1/3)



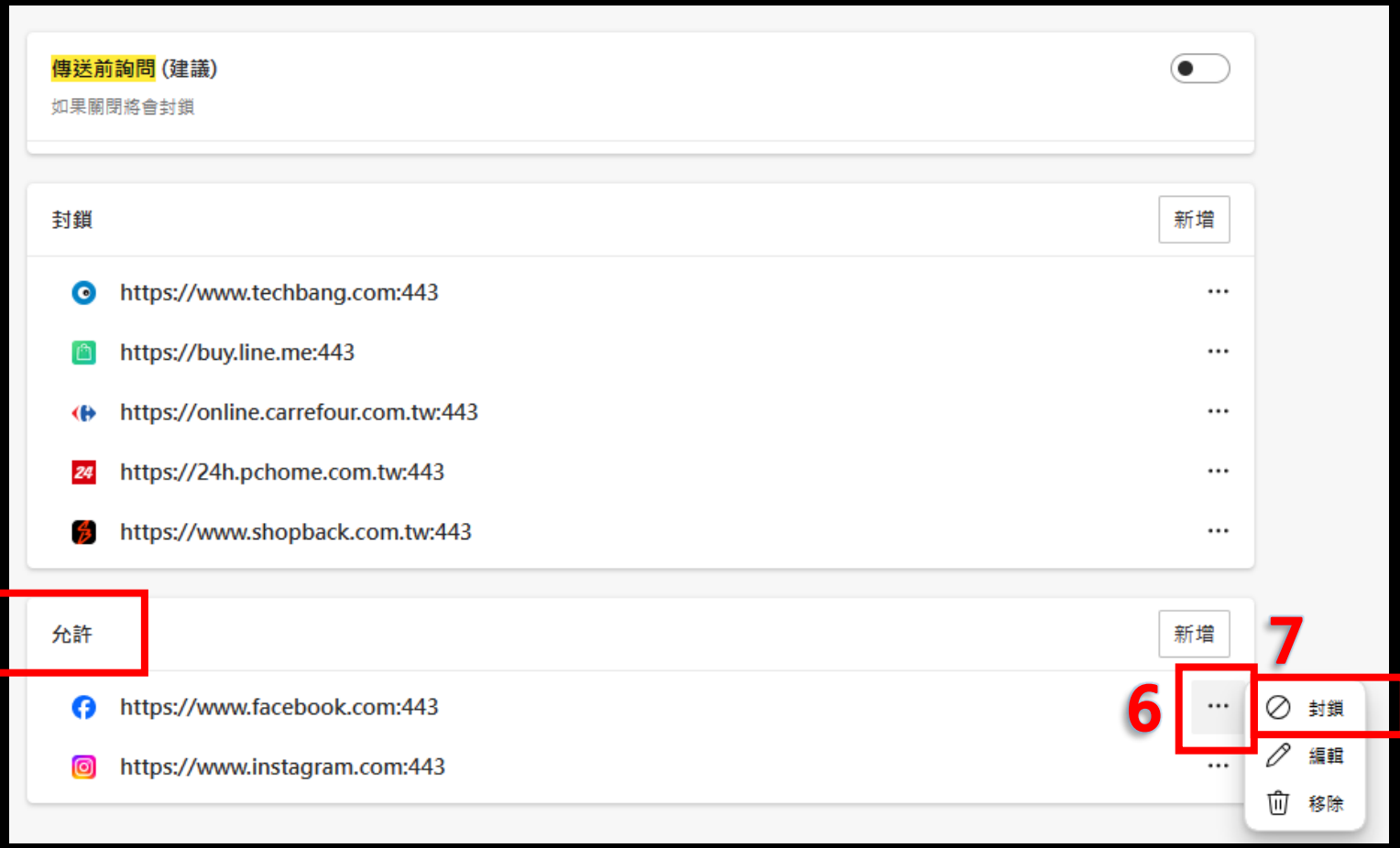
資安組關心您

#人員-Edge封鎖通知(2/3)



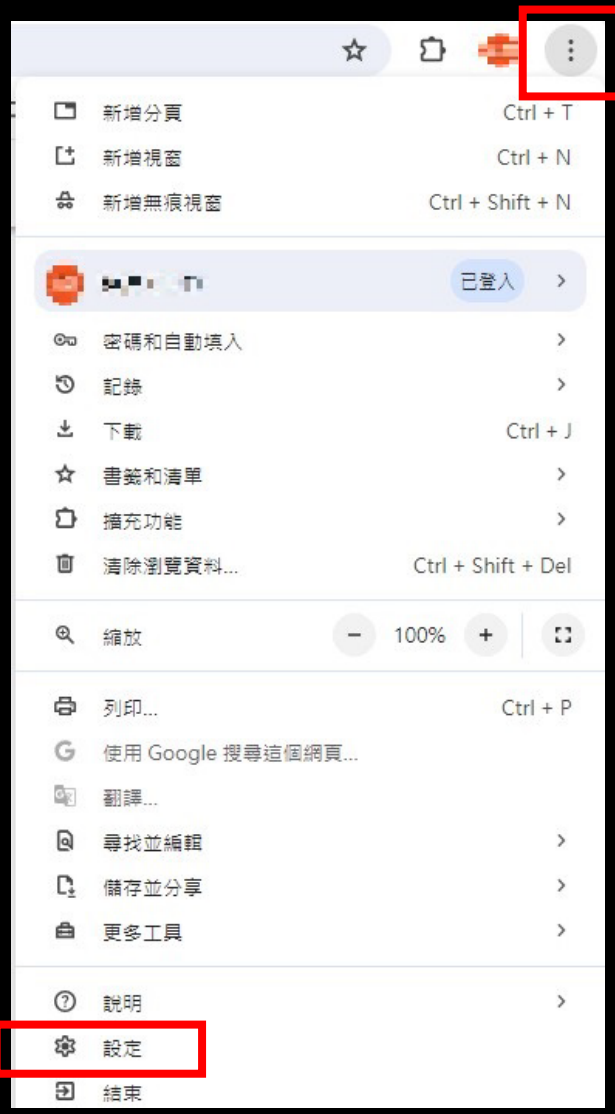
資安組關心您

#人員-Edge封鎖通知(3/3)



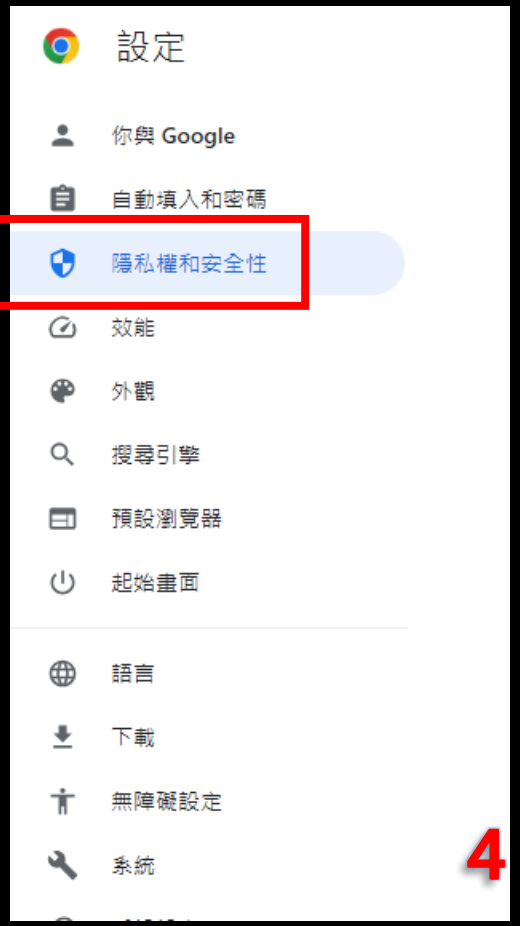
資安組關心您

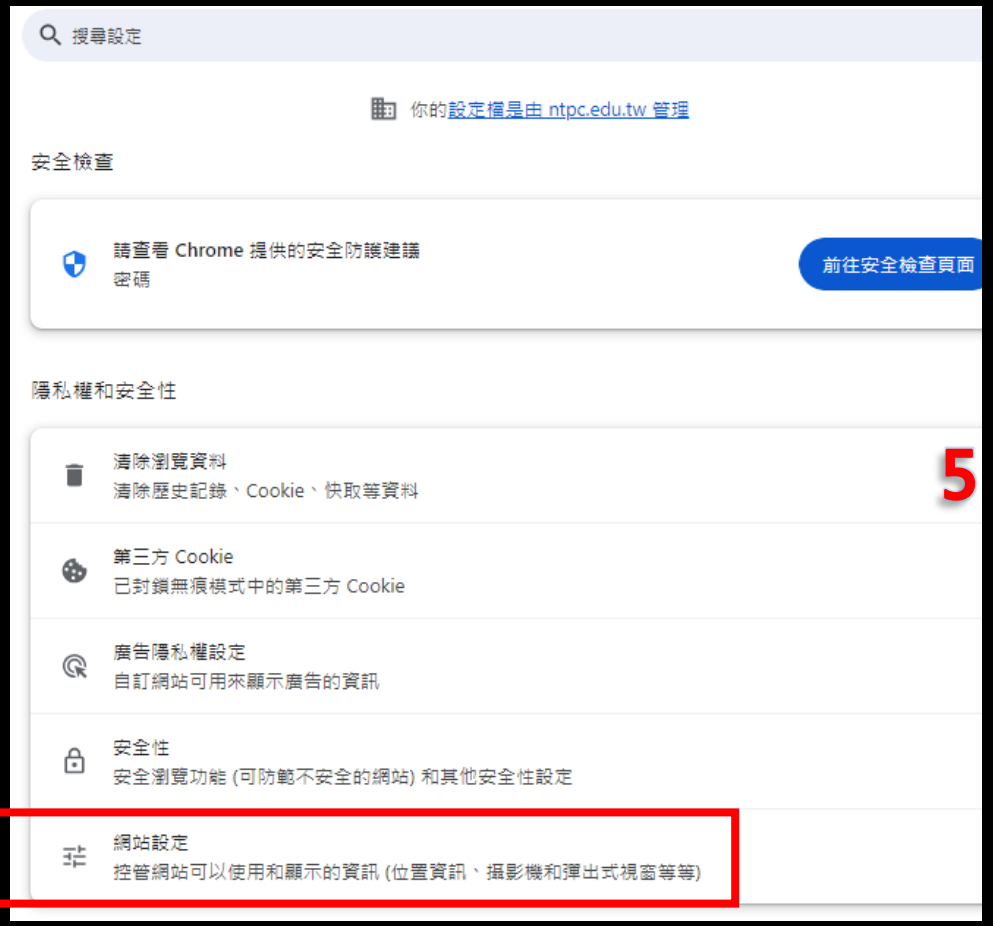
#人員-Chrome封鎖通知(1/3)

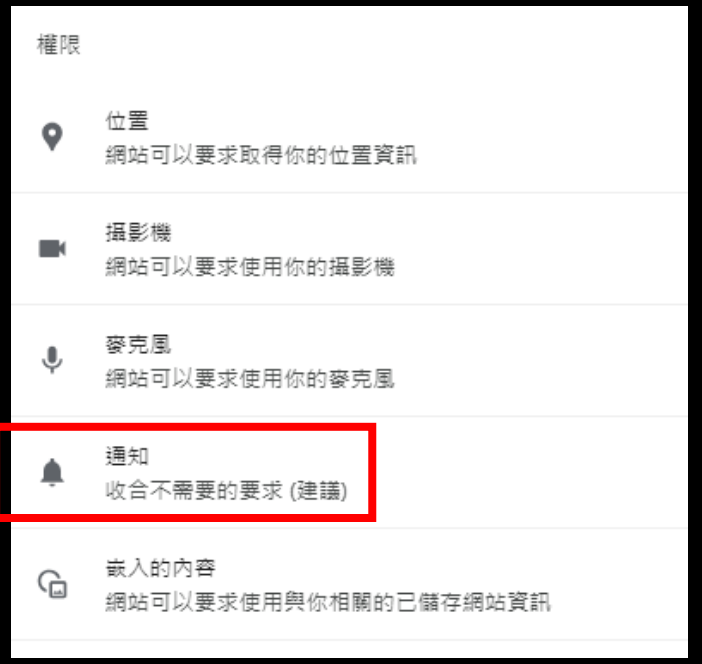


資安組關心您

#人員-Chrome封鎖通知(2/3)







資安組關心您

#人員-Chrome封鎖通知(3/3)

資安組關心您

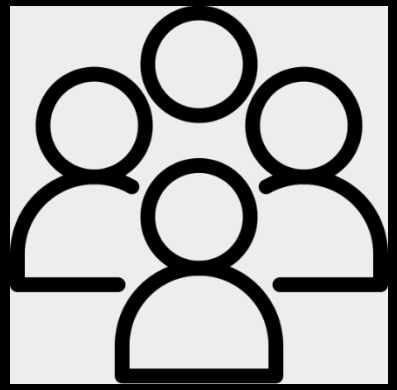
#實體

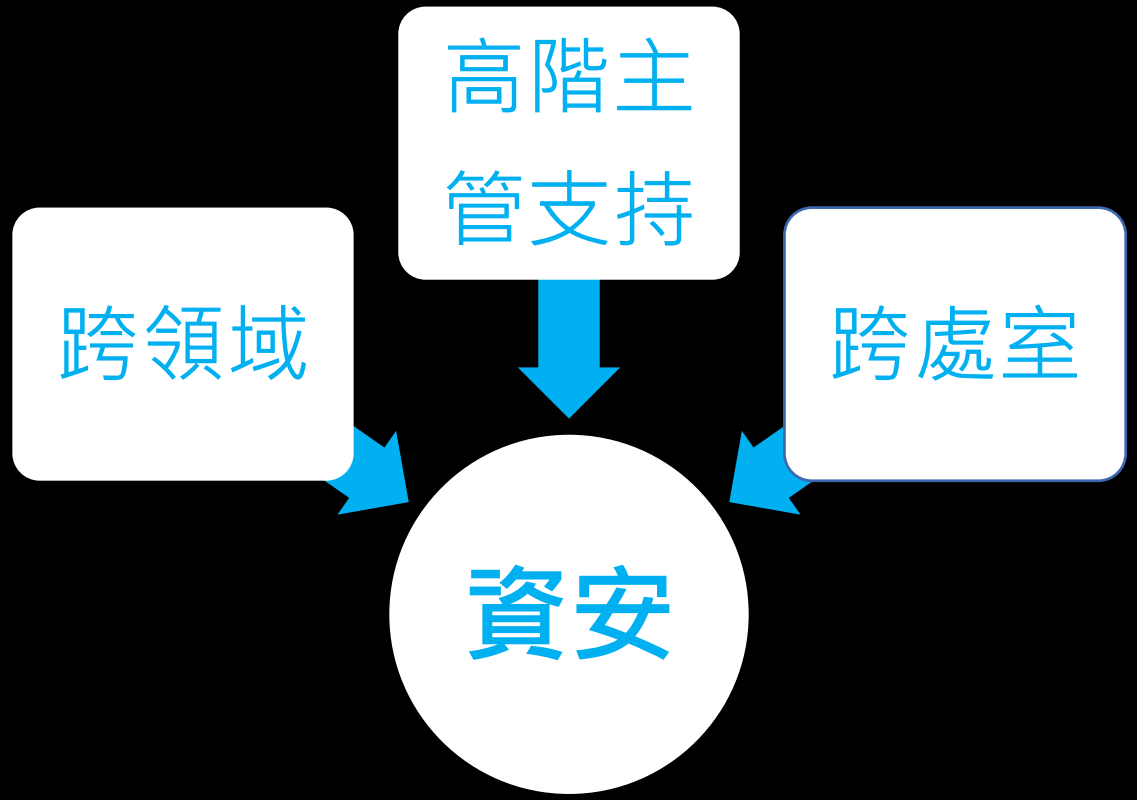
- 電腦有設密碼就安全嗎？
- 密碼建議9碼以上(大寫字母+ 小寫字母+ 數字+ 特殊符號)
- 離開座位鎖定電腦：Windows 標誌鍵 + L
- 帳密不要抄寫在電腦桌面附近
- 隨時注意可疑人物
- 符合消防法規
- 於安全區域內工作

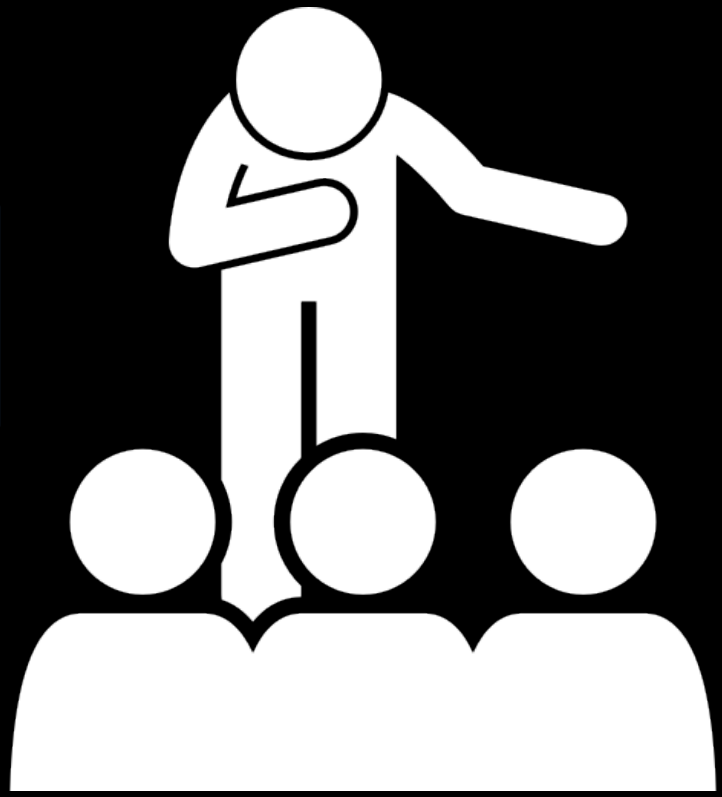
資安組關心您

#組織

- 資通安全維護計畫







資安組關心您