

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。

#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

#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

#技術-駭客駭入電腦第一件事

- Set-MpPreference -DisableRealtimeMonitoring \$true



Windows 安全性

←

☰

- 🏠 首頁
- 🛡️ 病毒與威脅防護
- 👤 帳戶防護
- 🔒 防火牆與網路保護
- 📁 應用程式與瀏覽器控制
- 📁 裝置安全性
- 📁 裝置效能與運作狀況

⚙️ 病毒與威脅防護設定

檢視及更新 Microsoft Defender 防毒軟體的病毒與威脅防護設定。

即時保護

找出及阻止惡意程式碼在您的裝置上安裝或執行。您可以暫時先關閉即時保護，稍後會為您自動重新開啟。

❌ 即時保護選項已關閉，讓您的裝置易受攻擊。

關閉

開啟即時保護以使用此功能。

有任何疑
取得協助

協助改善
提供我們

變更您的
檢視並變
的隱私權
隱私權設

#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」

病毒與威脅防護設定

檢視及更新 Microsoft Defender 防毒軟體的病毒與威脅防護設定。

即時保護

找出及阻止惡意程式碼在您的裝置上安裝或執行。您可以暫時先關閉即時保護，稍後會為您自動重新開啟。

開啟

開發人員磁碟機保護

在 [開發人員磁碟機] 磁碟區上以非同步方式掃描威脅，以減少對效能的影響。

病毒與威脅防護

保護您的裝置免受威脅。

Trend Micro Apex One 防毒

Trend Micro Apex One 防毒 已開啟。

目前的威脅

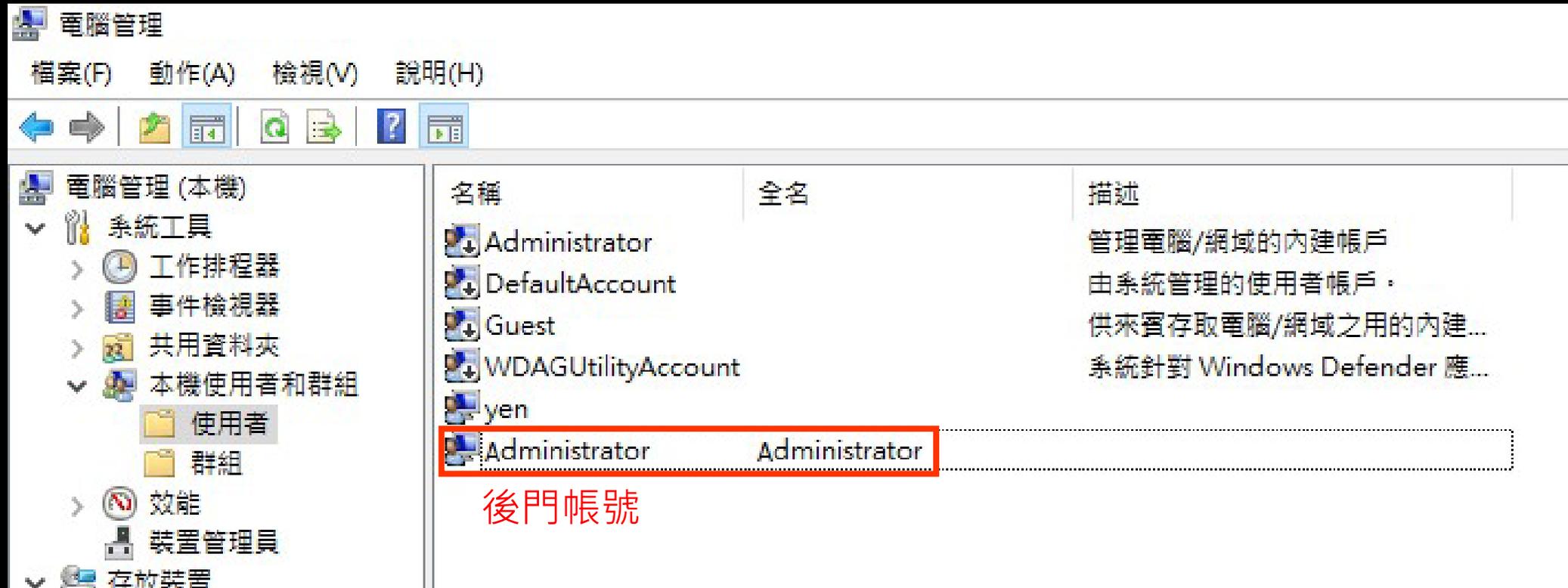
 不須採取動作。

保護設定

 不須採取動作。

#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」



The screenshot shows the Windows Computer Management console. The left pane shows the navigation tree with '本機使用者和群組' (Local Users and Groups) expanded to '使用者' (Users). The main pane displays a list of users with columns for '名稱' (Name), '全名' (Full Name), and '描述' (Description). The 'Administrator' user is highlighted with a red box, and the text '後門帳號' (Backdoor account) is written in red below it.

名稱	全名	描述
Administrator	Administrator	管理電腦/網域的內建帳戶
DefaultAccount		由系統管理的使用者帳戶，
Guest		供來賓存取電腦/網域之用的內建...
WDAGUtilityAccount		系統針對 Windows Defender 應...
yen		
Administrator	Administrator	

#技術-安裝集中式防毒並執行掃描

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



The screenshot shows the Taipei City Information Business Portal (新北市資訊業務入口網) website. The left sidebar contains a search bar and a navigation menu with the following items: 教資科資教股簡介, 資訊安全, 資安法規, 資安期程, 集中式防毒, and 資安資源. The main content area is titled '集中式防毒' (Centralized Antivirus) and includes the following text: '本市提供高中職、國中小及公立幼兒園(含契約期間新設立之所屬學校), 提供集中式防毒整合服務與授權, 由教網中心主動掌握各校則。' Below this, there are three links: '安裝方式: [集中式防毒安裝手冊](#)', '教育訓練: [防毒服務教育練簡報](#)', and '移除方式: 請洽各校資訊組長; 資訊組長請洽教網中心8072-3456#534.' At the bottom, there is a link for '備份321原則: [至少三份備份](#)'.

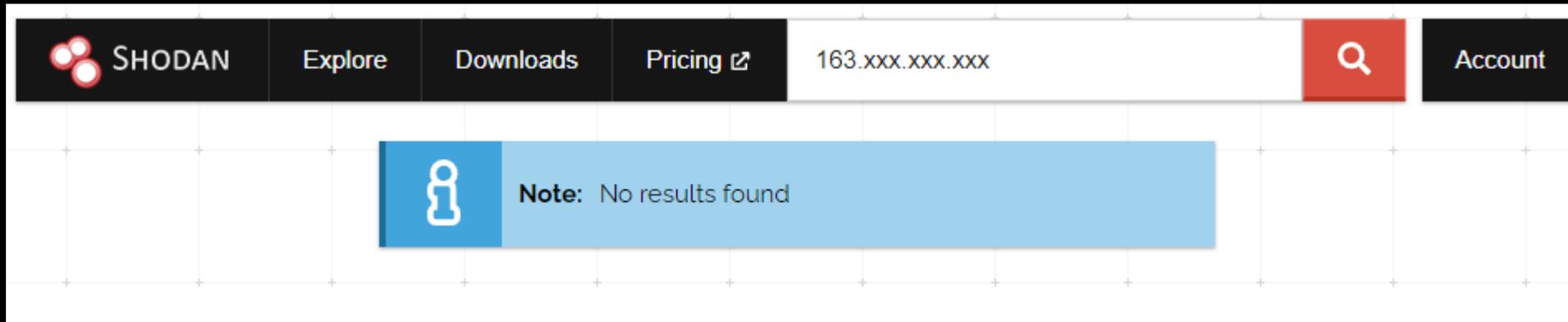
#技術-查詢自己IP位置

- 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)。

```
乙太網路卡 乙太網路 3:
    連線特定 DNS 尾碼 . . . . . : mshome.net
    描述 . . . . . : Microsoft Hyper-V Network Adapter #3
    實體位址 . . . . . : 00-15-5D-38-BF-0C
    DHCP 已啟用 . . . . . : 是
    自動設定啟用 . . . . . : 是
    連結-本機 IPv6 位址 . . . . . : fe80::1948:12b2:9576:bc8%10(偏好選項)
    IPv4 位址 . . . . . : 172.21.242.192(偏好選項)
    子網路遮罩 . . . . . : 255.255.240.0
    租用取得 . . . . . : 2024年4月29日 下午 04:02:16
    租用到期 . . . . . : 2024年4月30日 下午 04:02:16
    預設閘道 . . . . . : 172.21.240.1
    DHCP 伺服器 . . . . . : 172.21.240.1
    DHCPv6 IAID . . . . . : 234886493
    DHCPv6 用戶端 DUID. . . . . : 00-01-00-01-2D-B2-AC-84-00-15-5D-38-BF-09
    DNS 伺服器 . . . . . : 172.21.240.1
    NetBIOS over Tcpi . . . . . : 啟用
```

#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

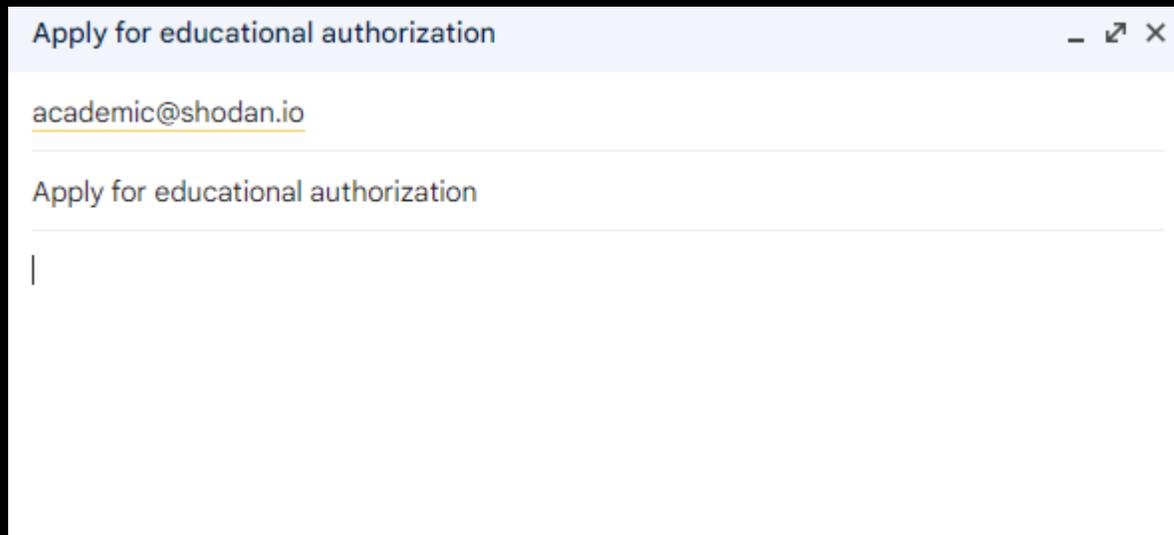


#技術- Shodan網段查詢

- <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」

#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

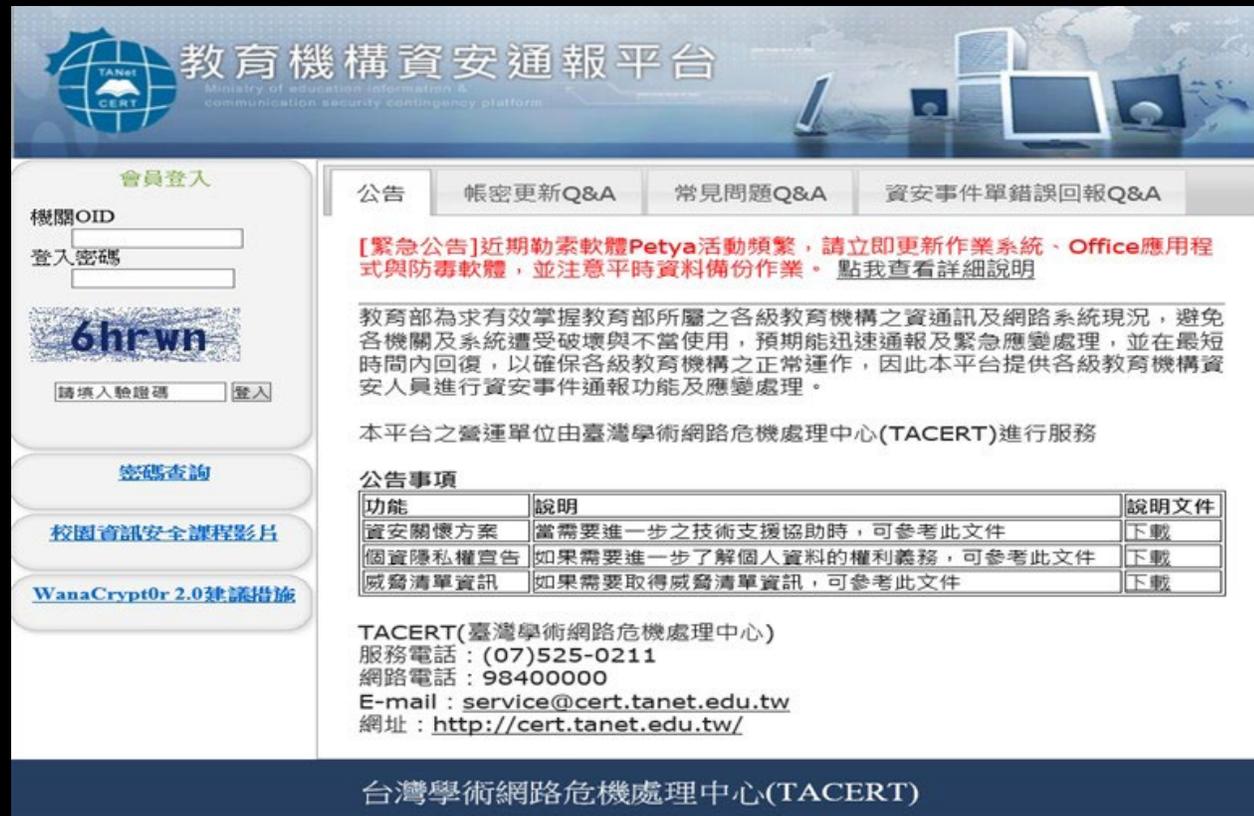


The screenshot shows an email composition window with the following details:

- Title:** Apply for educational authorization
- Recipient:** academic@shodan.io
- Subject:** Apply for educational authorization
- Body:** A large empty text area with a vertical cursor at the top left.

#技術-教育機構資安通報平台(1/4)

• <https://info.cert.tanet.edu.tw/prog/index.php>



教育機構資安通報平台
Ministry of Education Information & Communication Security Contingency Platform

會員登入

機關OID
登入密碼

6hr-wn

請填入驗證碼 登入

密碼查詢

校園資訊安全課程影片

WanaCrypt0r 2.0建議措施

公告 帳密更新Q&A 常見問題Q&A 資安事件單錯誤回報Q&A

[緊急公告]近期勒索軟體Petya活動頻繁，請立即更新作業系統、Office應用程式與防毒軟體，並注意平時資料備份作業。 [點我查看詳細說明](#)

教育部為求有效掌握教育部所屬之各級教育機構之資通訊及網路系統現況，避免各機關及系統遭受破壞與不當使用，預期能迅速通報及緊急應變處理，並在最短時間內回復，以確保各級教育機構之正常運作，因此本平台提供各級教育機構資安人員進行資安事件通報功能及應變處理。

本平台之營運單位由臺灣學術網路危機處理中心(TACERT)進行服務

公告事項

功能	說明	說明文件
資安關懷方案	當需要進一步之技術支援協助時，可參考此文件	下載
個資隱私權宣告	如果需要進一步了解個人資料的權利義務，可參考此文件	下載
威脅清單資訊	如果需要取得威脅清單資訊，可參考此文件	下載

TACERT(臺灣學術網路危機處理中心)
服務電話：(07)525-0211
網路電話：98400000
E-mail：service@cert.tanet.edu.tw
網址：<http://cert.tanet.edu.tw/>

台灣學術網路危機處理中心(TACERT)

- 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

#技術-教育機構資安通報平台(2/4)

The screenshot shows the user interface of the Education Institution Cybersecurity Reporting Platform. The header includes the TAnet CERT logo and the title '教育機構資安通報平台' (Education Institution Cybersecurity Reporting Platform). The main content area is divided into several sections:

- Unit Information (單位資訊):** Located at the top left, it contains fields for '機關名稱: 新北市' (Agency Name: New Taipei City) and '使用者:' (User:).
- Supervising Unit Information (主管單位資訊):** Located at the top center, it contains fields for '主管機關: 新北市教育網路中心' (Supervising Agency: New Taipei City Education Network Center), '聯絡電話: 02-8072-3456' (Contact Phone: 02-8072-3456), and 'E-Mail: ' (E-Mail:).
- Education Institution Unit Information (教育機構單位資訊):** Located at the top right, it contains fields for '教育機構資安通報應變小組' (Education Institution Cybersecurity Reporting Incident Response Team), '聯絡電話: 07-525-0211' (Contact Phone: 07-525-0211), and 'E-Mail: service@cert.tanet.edu.tw' (E-Mail: service@cert.tanet.edu.tw).
- Personal Information Area (個人資料區):** A vertical sidebar on the left containing navigation links: '回首頁' (Home), '修改個人資料' (Modify Personal Information), '登出' (Logout), and a '通報' (Reporting) section with sub-links: '通報/應變' (Reporting/Incident Response), '自行通報' (Self-reporting), '事件單處理狀態' (Event Single Processing Status), '歷史通報' (Historical Reporting), '帳號管理' (Account Management), '事件附檔下載' (Event Attachment Download), '資安預警事件' (Cybersecurity Warning Events), '事件統計' (Event Statistics), and '演練資訊' (Drill Information).
- Contact Information (聯絡資訊):** A central section containing contact details for the reporting center.
- Table:** A table with columns for '事件單編號' (Event Single Number), '發佈時間' (Release Time), '距通報時間(小時)' (Time since reporting (hours)), and '流程' (Process). The table is currently empty.

At the bottom of the page, the text '台灣學術網路危機處理中心(TACERT)' (Taiwan Academic Network Crisis Management Center (TACERT)) is displayed.

#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。

修改個人資料		
機關名稱	新北市	
帳號		
單位電話		
傳真		
地址		
聯絡人資料(1)		
聯絡人姓名		
職稱		
聯絡人電話		
聯絡人手機號碼		
聯絡人E-MAIL		
變更密碼		
目前密碼		
新密碼		
確認密碼		
送出	重填	
連絡人順序	連絡人名稱	連絡人EMAIL
第二連絡人		@ntpc.edu.tw

個人基本資料區

密碼變更區

單位其他
聯絡人資料區

#技術-教育機構資安通報平台(4/4)

工單狀態

事件單編號 搜尋

第一頁 . 上一頁 . 下一頁 . 最終頁

事件編號	發佈編號	單位	IP	LOG附檔
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	下載
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	下載
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	下載
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	下載
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	下載

Page 153/153

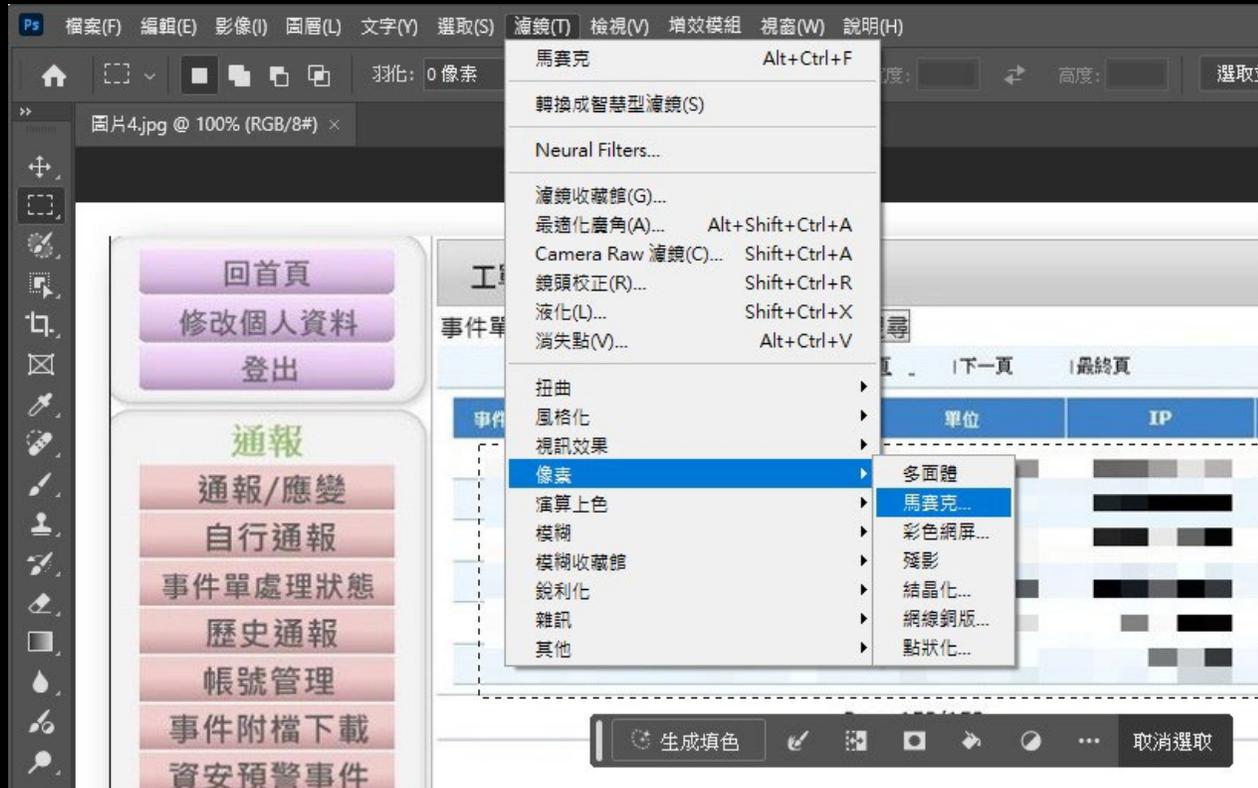
台灣學術網路危機處理中心(TACERT)

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

#技術-遮罩

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



#技術-VPN

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

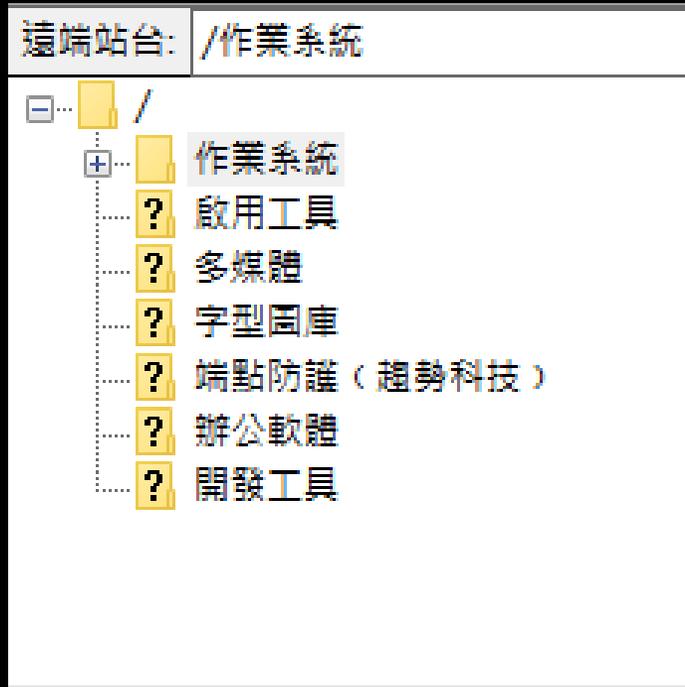
新北市親師生平台

◀ 市集 近期活動專區 閱讀專區 新北市專區 教i ▶

各級學校網站	新北市立圖書館電子資源	「來註冊」數位教學平台	校園食材履歷追溯
 資訊教育論壇	 生活英語動起來	 橋點趣教室	 新北電競王 (夢幻果島大冒險)
 能源教育平台 (測試中)	 資安業務管理	 會考e點靈	 教育資料平台
 自編雙語教材	 智慧命題系統	 奧多比軟體授權網	 校舍管理系統 (測試中)
 新北星聯盟 (數位星球)	 虛擬私有網路服務		

#技術-FTP

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



#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？

#人員-駭客？(1/4)



#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。

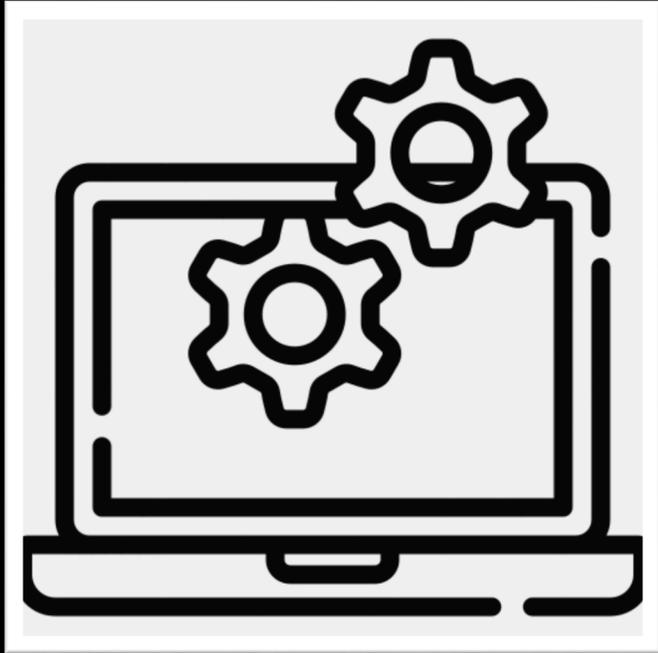
ex:伊朗核電廠 stuxnet

#人員-駭客？(3/4)

- 經「授權」
才是「白帽駭客」。



#人員-駭客？(4/4)



技術



興趣



特質

#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/>

#人員-提升資安素養



#人員-提升資安素養



#人員-提升資安素養

電腦被勒索 煩惱多更多



#人員-提升資安素養



網路使用要注意 資通安全沒煩惱

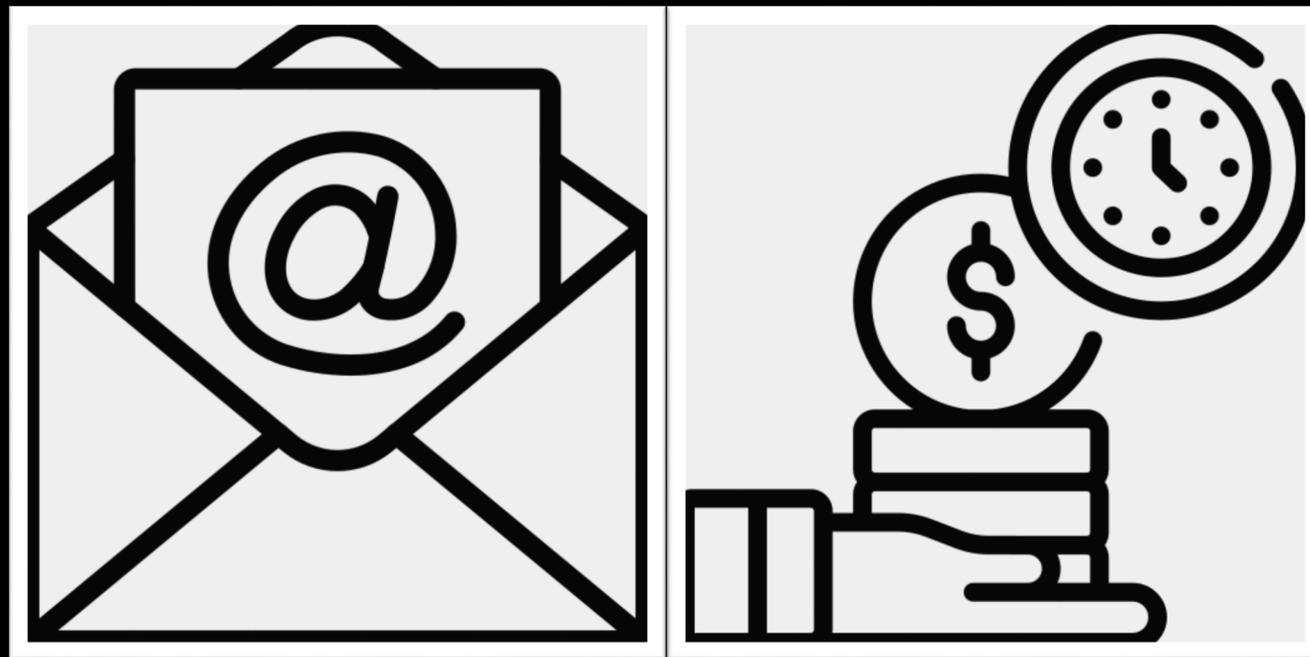


#人員-社交工程



滲透

VS



社交工程

#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>

#人員-郵件標題無法判斷(1/2)

郵件標題

小提醒：郵件標題**無法判斷**是否為社交工程信件

1. 開啟信件前**先檢查寄件者地址**，非公務信箱網域結尾請提高警覺
(常見公務信箱網域結尾：**GOV.TW**或**EDU.TW**)
2. **與公務無關請勿開啟**，看似與公務相關仍須保持警覺
(首次通信前可與寄件者先電話聯繫)

▼下列為曾經出現過的社交工程信件標題▼

#人員-郵件標題無法判斷(2/2)



#人員-實際釣魚郵件案例(1/2)



#人員-非社交工程電子郵件案例(1/2)



#人員-非社交工程電子郵件案例(2/2)



#人員-防範社交工程郵件_純文字模式

Openfind™ MAIL2000 強化郵件軟體安全設定「webmail.ntpc.edu.tw」：

使用環境

1 個人設定

2 個人化設定

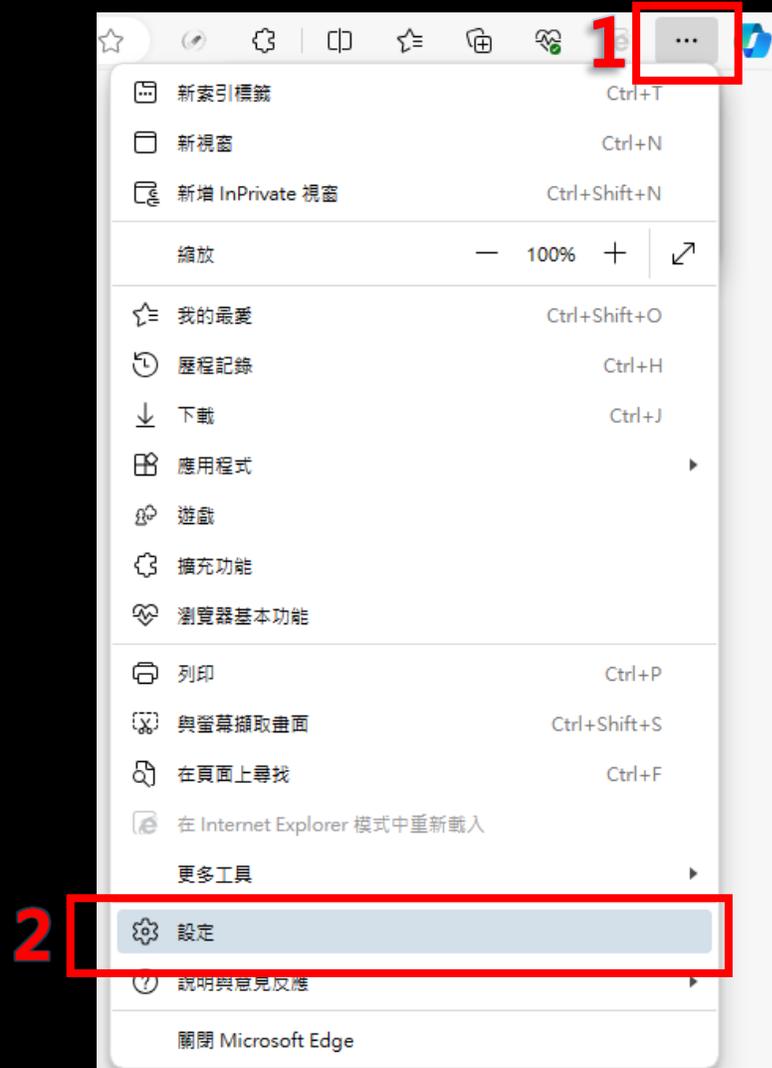
3 使用環境

4 郵件

5 信件自動預覽 關閉 開啟
預設讀信方式 純文字
封鎖外部圖檔 全部封鎖
內文圖片要封鎖
已讀信件不封鎖
好友信件不封鎖

6 確定 取消

#人員-Edge封鎖通知(1/3)



#人員-Edge封鎖通知(2/3)

3

設定

傳送前詢問

- 個人檔案
- 隱私權與安全性
- 搜尋與服務
- 外觀
- 側邊欄
- 開始、首頁及新索引標籤
- 分享、複製並貼上
- Cookie 和網站權限
- 預設瀏覽器
- 下載
- 家長監護服務
- 語言

所有存取權限

在所有網站上套用的權限

- 位置
先詢問
- 相機
先詢問
- 麥克風
先詢問
- 動作或光感應器
允許網站使用動態和光感應器
- 1 個結果**
通知
已封鎖
- JavaScript
已允許

4

#人員-Edge封鎖通知(3/3)

傳送前詢問 (建議)

如果關閉將會封鎖

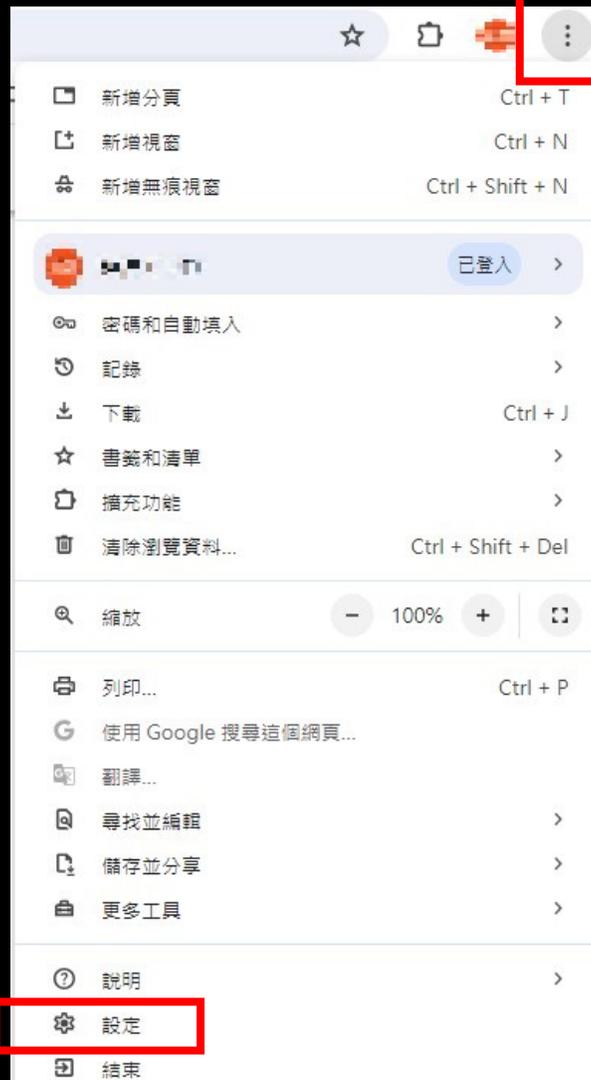
封鎖 新增

-  <https://www.techbang.com:443> ...
-  <https://buy.line.me:443> ...
-  <https://online.carrefour.com.tw:443> ...
-  <https://24h.pchome.com.tw:443> ...
-  <https://www.shopback.com.tw:443> ...

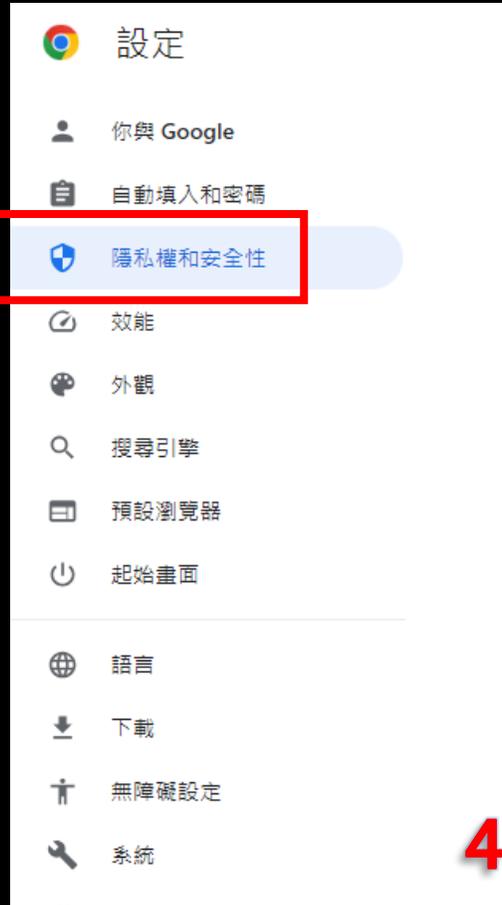
5 **允許** 新增 **7**

-  <https://www.facebook.com:443> **6** ... 封鎖
-  <https://www.instagram.com:443> ... 編輯
- ... 移除

#人員-Chrome封鎖通知(1/3)



#人員-Chrome封鎖通知(2/3)



3

- 設定
- 你與 Google
- 自動填入和密碼
- 隱私權和安全性**
- 效能
- 外觀
- 搜尋引擎
- 預設瀏覽器
- 起始畫面
- 語言
- 下載
- 無障礙設定
- 系統

4



搜尋設定

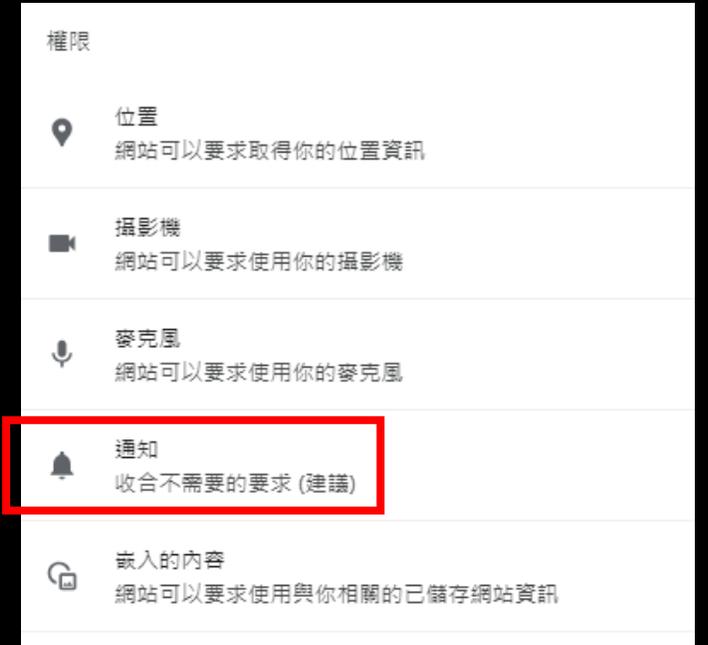
你的設定權是由 ntpc.edu.tw 管理

安全檢查

請查看 Chrome 提供的安全防護建議密碼 [前往安全檢查頁面](#)

隱私權和安全性

- 清除瀏覽資料
清除歷史記錄、Cookie、快取等資料
- 5 第三方 Cookie
已封鎖無痕模式中的第三方 Cookie
- 廣告隱私權設定
自訂網站可用來顯示廣告的資訊
- 安全性
安全瀏覽功能 (可防範不安全的網站) 和其他安全性設定
- 網站設定**
控管網站可以使用和顯示的資訊 (位置資訊、攝影機和彈出式視窗等等)



權限

- 位置
網站可以要求取得你的位置資訊
- 攝影機
網站可以要求使用你的攝影機
- 麥克風
網站可以要求使用你的麥克風
- 通知**
收合不需要的要求 (建議)
- 嵌入的內容
網站可以要求使用與你相關的已儲存網站資訊

#人員-Chrome封鎖通知(3/3)

自訂設定

下列網站採用自訂設定，而非預設設定

不允許傳送通知 新增

-  <https://meet.google.com:443> 已自動封鎖
-  <https://www.mobile01.com:443> 已自動封鎖
-  <https://www.bnext.com.tw:443> 已自動封鎖
-  <https://pts.ntpc.edu.tw:443>

6

允許傳送通知 新增

-  <https://www.facebook.com:443>
-  <https://drive.google.com:443>

7

8

封鎖

編輯

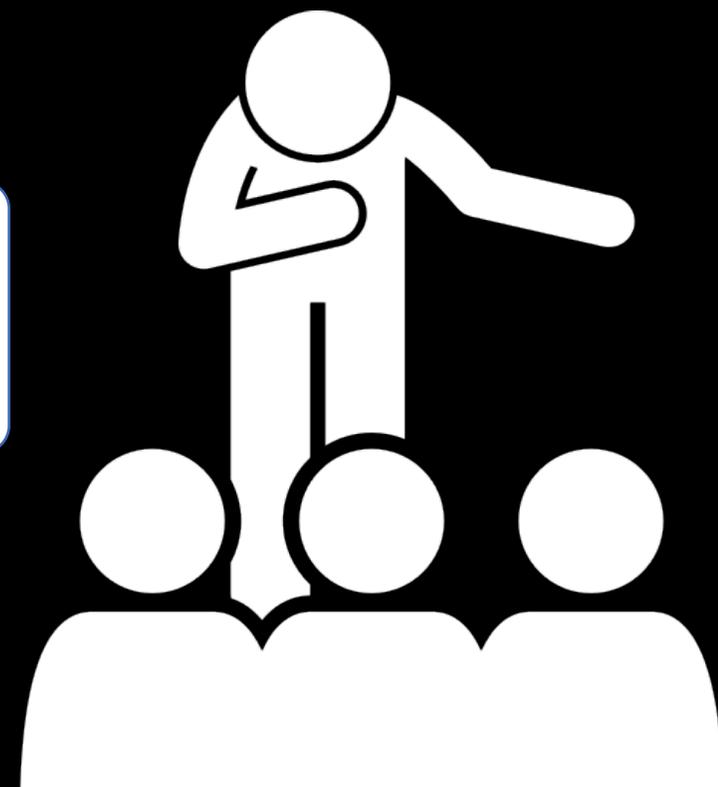
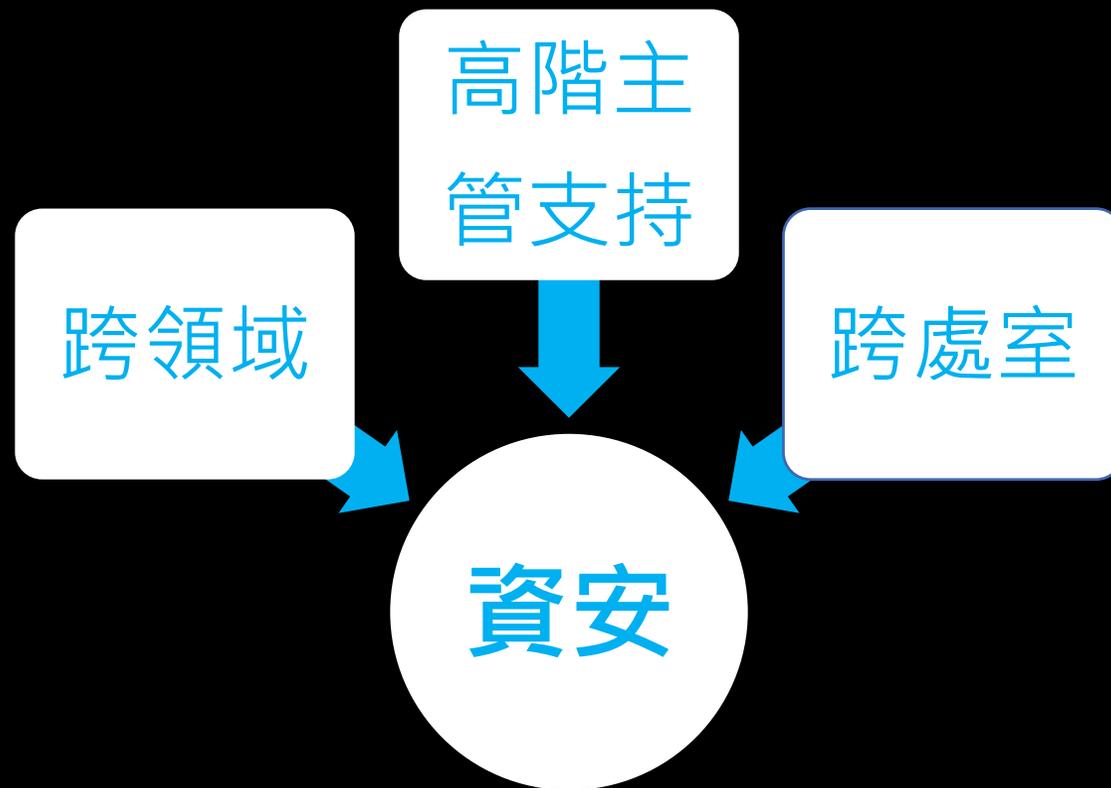
移除

#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

#組織

- 資通安全維護計畫



資安組關心您♥