

# 臺南市政府 筆硯文書編輯系統 系統管理者教育訓練 資訊安全宣導

109年09月

# 大綱

- 系統帳號及權限管理注意事項說明
- 資訊安全宣導說明
  1. 維護資訊安全的重要作法
  2. 問題發生時的處理方法
  3. 惡意程式感染時的處理方法
  4. 資安風險類別
  5. 個人電腦的資訊安全

---

# 系統帳號及權限管理注意事項說明

# 本府ISMS要求

## ➤ 管理規範：

### ISMS-03-11 帳號註冊註銷作業程序書V1.1

## ➤ 權責：

1. 系統使用者之權限設定、變更、停用等作業，由各機關(單位)及學校之**系統管理者**負責管制及設定，若有帳號或權限需新增及調整時，請填寫「ISMS-04-07 帳號新增或異動申請單V1.2」後異動。
2. 系統管理者請定期(週期為**每半年一次**)清查內部相關帳號及權限設定(請填寫ISMS-04-42+帳號清查紀錄表V1.1)，確認是否為機關的使用者。
3. 本府會定期(週期為**每半年一次**)函文請各機關(單位)及學校確認系統管理者帳號及權限設定，確認是否為現任中的系統管理者。

---

# 資訊安全宣導說明

## 說明

1. 筆硯文書編輯系統帳號及密碼設定應遵循本府帳號密碼之相關安全規定。(帳號請勿使用身分證字號為登入帳號)
2. 個人電腦作業系統應定期進行漏洞修補。
3. 安裝防毒軟體，並定期更新病毒碼，對於承辦公文及其附件進行掃描，偵測有無感染電腦病毒。
4. 公務電腦請勿使用網路芳鄰或安裝點對點 (P2P)、即時通訊(IM)、社交軟體等網路應用程式，以杜絕任何惡意程式可能之入侵管道。
5. 公務電腦應定期執行備份作業，以確保個人電腦系統安全。

# 維護資訊安全的重要作法

- 使用安全的密碼並定期更換。
- 不在網站留下個人私密資料與密碼。
- 強化瀏覽器選項安全設定。
- 不輕易執行、開啟來路不明的檔案。
- 重要檔案加密處理。
- 備份重要檔案資料。
- 使用個人防火牆保護電腦。
- 定期更新修補軟體漏洞。
- 使用防毒軟體並隨時更新病毒碼。
- 謹慎使用可攜式設備、儲存媒體。

# 問題發生時的處理方法

當我們面對一個被駭、受感染的工作站或是其他緊急事件時；要保持冷靜且遵守正確的步驟來處理。以下有八個步驟可以應付大部份的緊急事件：

- 1) 不要驚慌
- 2) 了解狀況
- 3) 與資訊(安)部門保持聯絡
- 4) 將傷害降到最低
- 5) 採取適當的回復步驟
- 6) 針對狀況來做適當的回應
- 7) 記取教訓
- 8) 保持冷靜且小心操作

# 惡意程式感染時的處理方法(1/3)

對於惡意程式的感染，以下步驟可以應付大部份的危險狀況。

## 1) 確認感染

並不是每次電腦怪怪的就一定是因為中毒，可以透過防毒軟體確認系統是否中毒。如果無法100%確定，那還是謹慎一點，尋求幫助。

## 2) 控制感染狀況

把系統的網路關掉。拔掉網路電纜、或關掉WI-FI，然後把系統關機直到你可以用安全的方式來開機作往後的處理。以防止病毒去毀掉電腦上更多資料或是散播到其他電腦或寄發垃圾郵件。

# 惡意程式感染時的處理方法(2/3)

## 3) 確認處理步驟的方向

許多管理員為了以防萬一，都採取清空整個系統來避免更多的傷害，而不想冒險只去清除受感染的檔案。但硬碟中或許還存有重要資料需要備份。我們需要好好考慮是否要整個清空或是先做備份。

## 4) 嘗試清理系統

要確定我們可以靠著安全的方式來開機，這樣才不會再度啟動已經受到感染的應用程式。

# 惡意程式感染時的處理方法(3/3)

## 5) 經常做還原點的儲存

如果無法保證能把系統清理乾淨，但是卻有作完整的還原紀錄。那就根據之前的還原紀錄來作系統還原。

## 6) 重新建立系統

如果無法清理乾淨或是還原，那麼別無選擇只好從頭把系統重新建立起來。先備份重要資料，再把整個系統完全格式化後再作安裝。

## 7) 記取教訓

解決問題後，找出惡意程式穿越防禦的原因，把缺陷記錄下來，減少再度發生的可能性。

# 資安風險類別-網路釣魚(1/3)

## ➤ 網路釣魚

### 1. 什麼是網路釣魚

- 以假網站冒充真網站引誘消費者上勾，騙取帳號、通行碼、信用卡、網路銀行帳號...等資料

### 2. 釣魚網站(偽冒網站)

- 駭客註冊網域名稱與「正牌」之真正網域名稱極為相似，利用極為相似之字母或數字，使上網之民眾難以辨別真偽，而誤觸駭客之網路釣魚陷阱。如：[www.hinet1.net](http://www.hinet1.net)、[www.micr0s0ft.com](http://www.micr0s0ft.com)
- 購買網路關鍵字廣告服務並於各大入口網站搜尋行銷服務刊登「關鍵字廣告」，使用者上網搜尋「網路銀行」等條件時，搜尋結果的最上方即出現犯罪集團之「關鍵字廣告」

### 3. 釣魚網站(網頁掛馬)

- 當使用者點選疑似「正牌」之網站後，駭客利用暗藏網頁框架夾藏惡意程式碼，以隱藏方式指向連結至其他網站之網頁空間，執行駭客預先上傳之木馬程式，讓使用者沒有感覺任何異樣，但是實際上下載多個木馬程式至使用者的個人電腦

# 資安風險類別-網路釣魚(2/3)

## ➤ 辨別釣魚網站

1. 魚目混珠的網址：可利用不同的搜尋引擎、whois查詢，多方確認
2. 以e-mail假通知信，提供假超連結：注意連結的網址
3. 參考公正單位發放的可信賴標章：如經濟部、台北市新聞處的可信賴電子商店標章



# 資安風險類別-網路釣魚(3/3)

## ➤ 有效分辨「網路釣魚」郵件方式

1. 發信人的名稱或郵件地址
  - 是否有異常？需確認發信者的身分
2. 電子郵件的主旨與內容
  - 與本身的工作、業務是否有關連
3. 網頁連結或夾帶附件檔案是否可疑
  - 郵件內異常網址連結判斷
  - 附加檔案之檢查

# 資安風險類別-電子郵件(1/3)

## ➤ E-mail攻擊

1. 運用有趣或熱門新聞事件為主旨寄發電子郵件，內容夾帶如下：
  - ① 惡意程式的附件
  - ② 惡意的連結或釣魚網站
  - ③ 假冒寄件者
  - ④ 假冒數位簽章ID
2. 社交工程手法—透過E-mail或電話方式騙取敏感資訊或測試使用者之資安認知能力。

# 資安風險類別-電子郵件(2/3)

## ➤ 對於電子郵件應有警覺性

### 1. 「為何我會收到這封郵件」

- 寄件來源

### 2. 「我是否應該收到這封郵件」

- 郵件主旨
- 郵件內容

### 3. 「我是否應該開啟這封郵件」

- 是否業務或工作需要
- 不開啟或不點選連結是否有影響
- 評估可接受之風險
- 審慎查證

### 4. 對於切身相關的電子郵件，若內含威脅、利誘、警告、提示等訊息內容，先思考後再行動作，應考慮詐騙之可能性

# 資安風險類別-電子郵件(3/3)

## ➤ 有效防範社交工程郵件的方式

1. 不點選不明電子郵件內含之URL或IP地址連結
2. 不開啟不明電子郵件及附件檔案
3. 個人資訊勿隨意登錄於不明網站
4. E-mail 管理
  - 區分公司及個人使用之信箱
    - E-Mail 帳號避免大眾化名稱
  - 不常使用之信箱，用於網站會員或其他服務之註冊
    - 專收垃圾信件
  - 在外登錄使用之信箱，將收到許多垃圾郵件，使用時務必小心
5. 不回覆來源不明之郵件
6. 勿讀取不明來源（垃圾）郵件
7. 關閉郵件預設瀏覽之設定

# 資安風險類別-即時通訊等

## ➤ 即時通訊

1. 偽造超連結：主機中毒後發送具有惡意程式的超連結至所有的聯絡人，誘使其他聯絡人好奇點選，進而植入木馬程式，再重複散播至更多使用者。

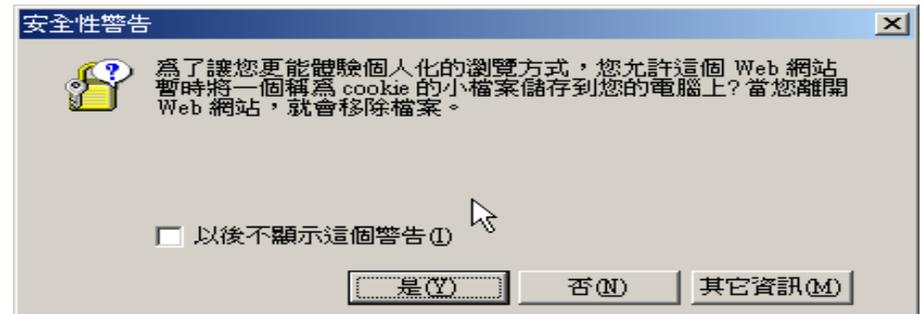
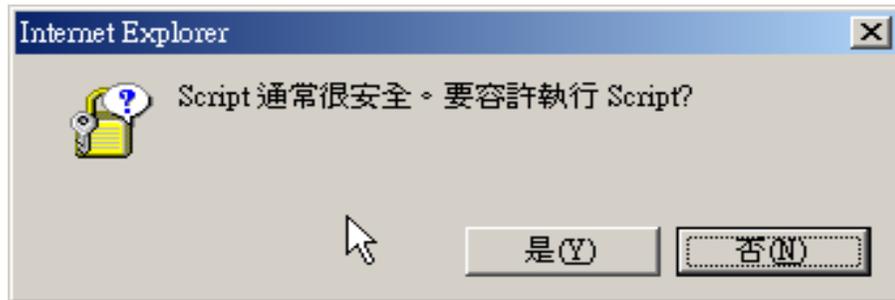
## ➤ 討論區或部落格

- 偽造超連結：在網站上留下具有惡意程式的超連結，誘騙使用者點選，植入木馬程式。

# 個人電腦的資訊安全(1/10)

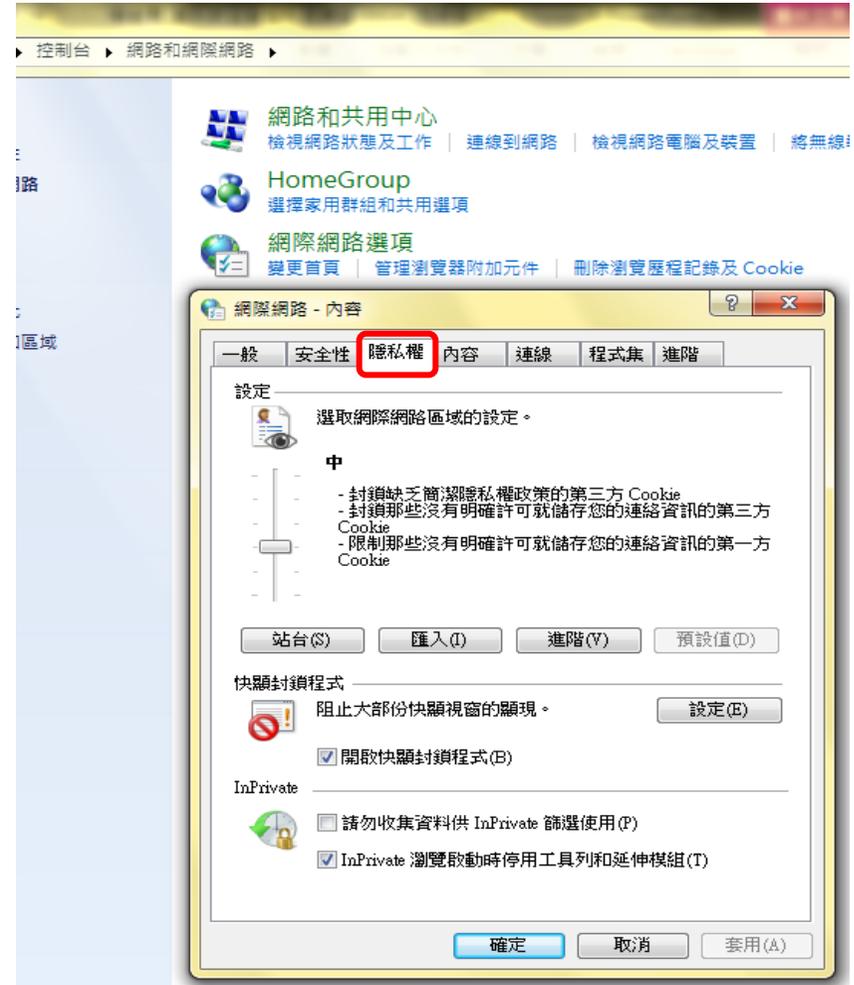
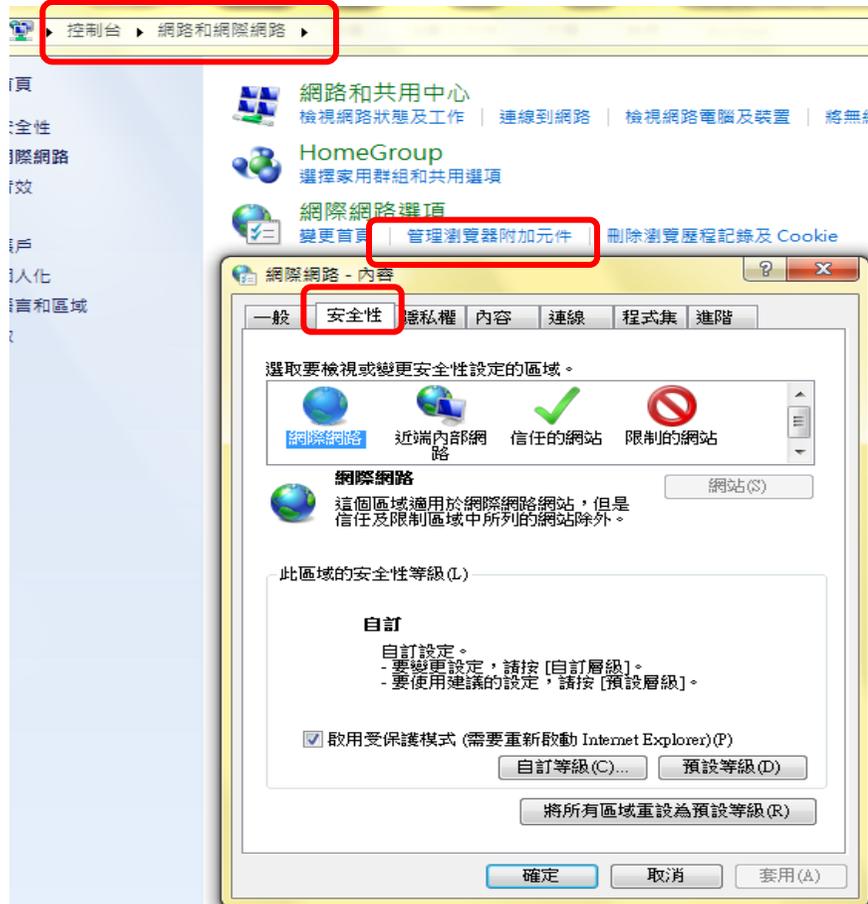
## ➤ 瀏覽網際網路的安全

1. **Script**：允許對方網站透過IE在電腦中執行指令
2. **Cookie**：允許對方網站在電腦中記錄與讀取資訊
3. **ActiveX**：允許對方網站在你的電腦執行程式



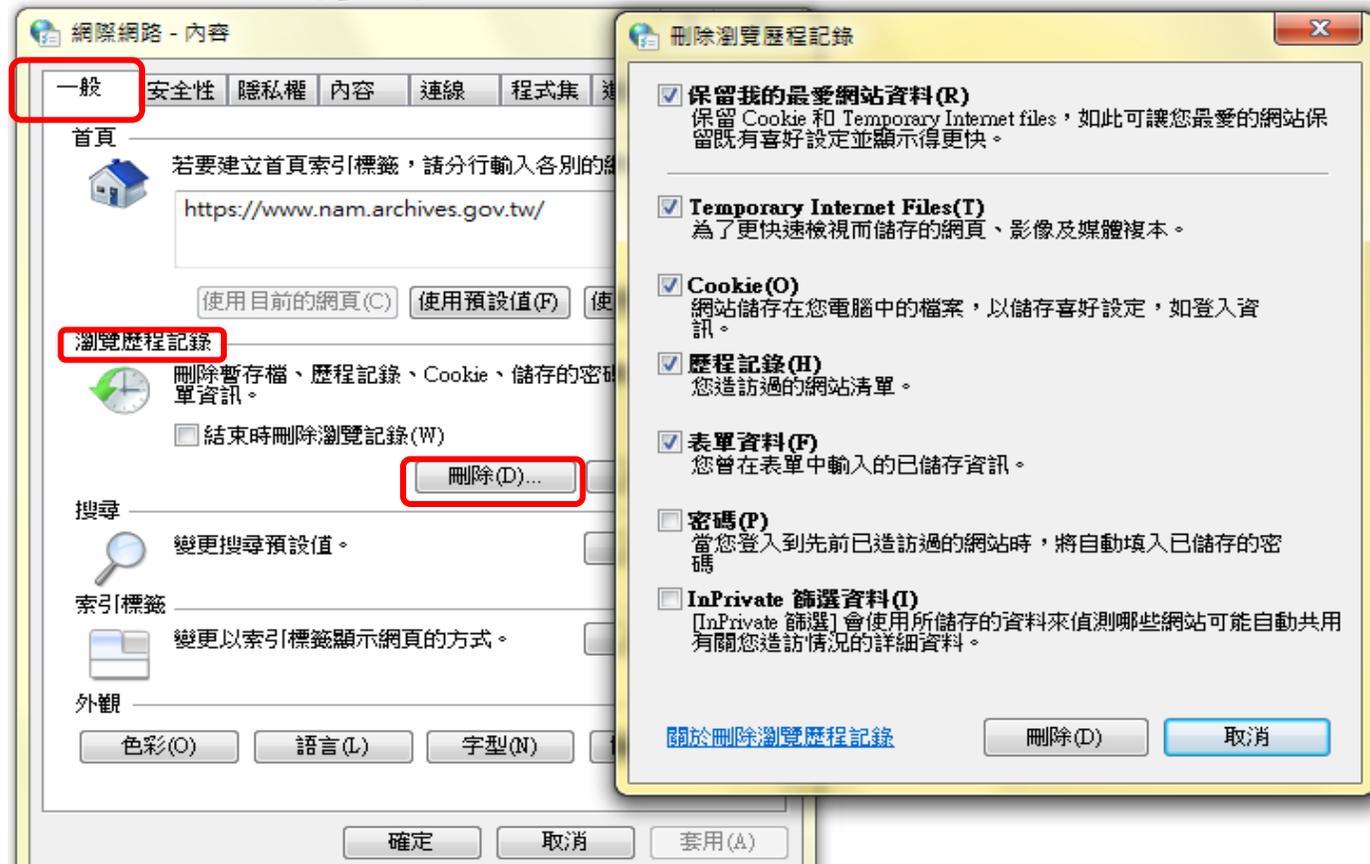
# 個人電腦的資訊安全(2/10)

## ➤ IE安全性設定



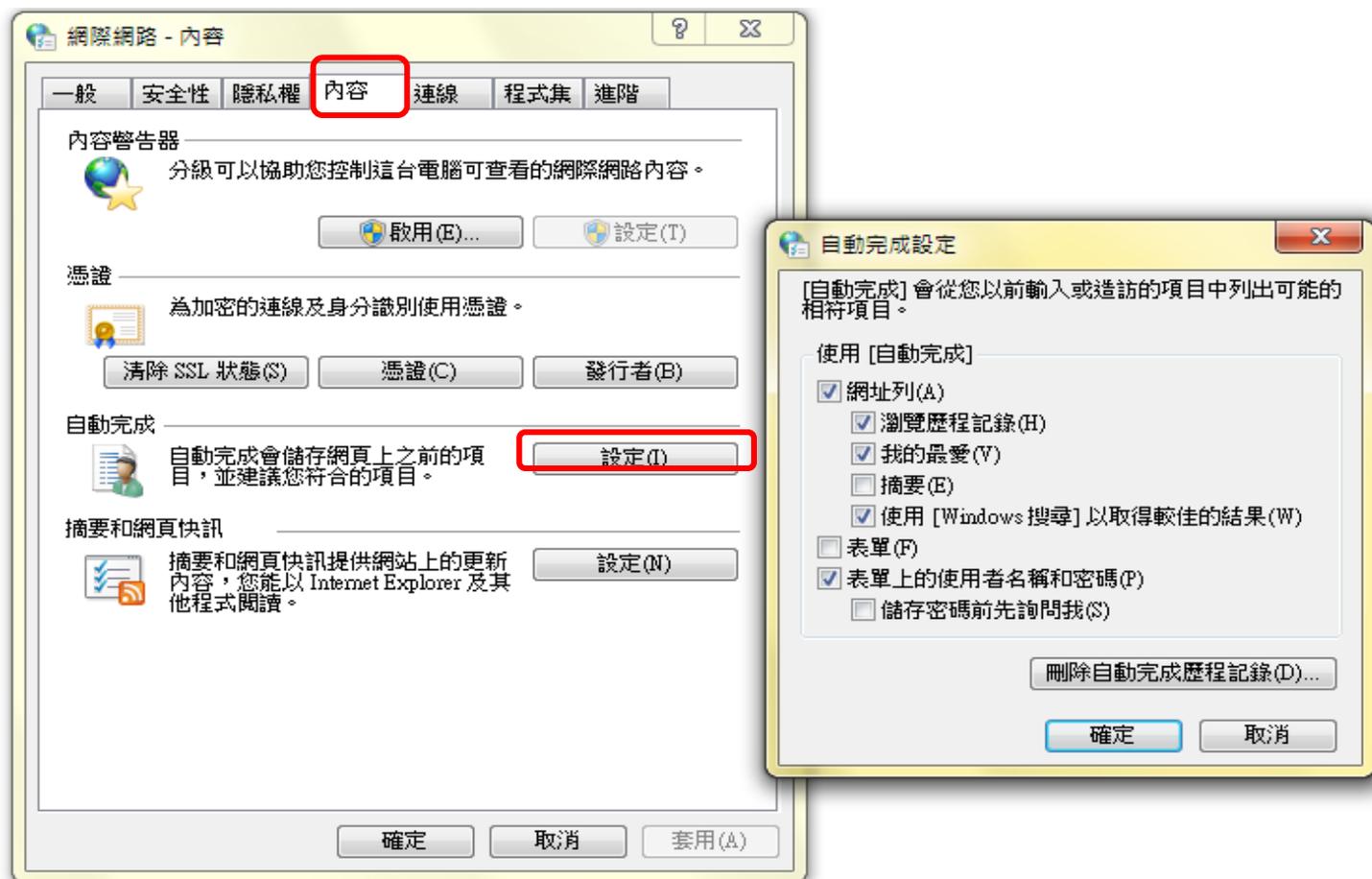
# 個人電腦的資訊安全(3/10)

## ➤ Cookie清除



# 個人電腦的資訊安全(4/10)

## ➤ IE自動完成帳號密碼的清除



# 個人電腦的資訊安全(5/10)

## ➤ E-mail的安全

### 1. 什麼是垃圾郵件？

- 不明人士寄的廣告信、無意義之信或匿名、冒名寄來的信

### 2. 關閉郵件預覽功能

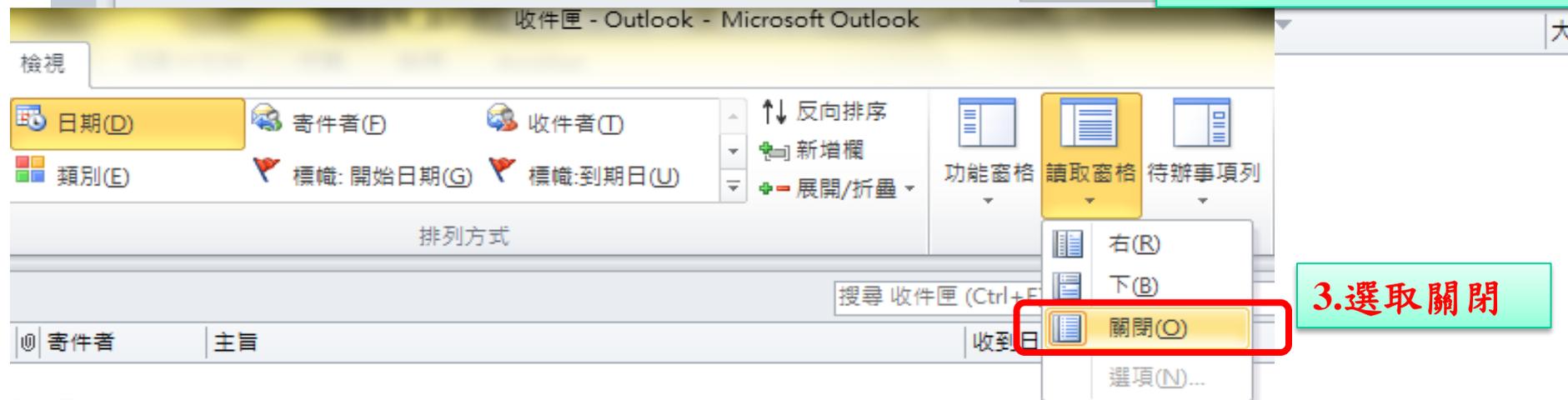
- 勿輕易讓自己的電子郵件信箱曝光
- 不明來源之郵件應避免回信，勿開啟直接刪除
- 勿到不知名的網站註冊登記自己的電子郵件信箱
- 收到轉寄信件勿隨再轉寄，必須轉寄信件給多人時應刪除原寄件者資訊
- 使用密件副本，保護收信人隱私
- 轉寄前應查證信件內容的正確性
- 勿將前寄件人的收信名單引入信件中
- 關閉Outlook Express預覽功能

# 個人電腦的資訊安全(6/10)

## ➤ Outlook 預覽功能關閉



2. 選取版面配置：讀取視窗



月: 今天

# 個人電腦的資訊安全(7/10)

## ➤ Windows個人防火牆

1. Windows 7具有簡易防火牆系統
2. 開啟防火牆
3. 設定可以連線的服務
4. 設定例外的允許連線情形
5. 查看記錄



### 網域網路位置設定

- 開啟 Windows 防火牆
- 封鎖所有連入連線，包括允許的程式清單中的連入連線
- 當 Windows 防火牆封鎖新的程式時請通知我

- 關閉 Windows 防火牆 (不建議)

### 家用或工作場所 (私人) 網路位置設定

- 開啟 Windows 防火牆
- 封鎖所有連入連線，包括允許的程式清單中的連入連線
- 當 Windows 防火牆封鎖新的程式時請通知我

- 關閉 Windows 防火牆 (不建議)

### 公用網路位置設定

- 開啟 Windows 防火牆
- 封鎖所有連入連線，包括允許的程式清單中的連入連線
- 當 Windows 防火牆封鎖新的程式時請通知我

- 關閉 Windows 防火牆 (不建議)

# 個人電腦的資訊安全(8/10)

## ➤ 病毒防護

1. 防毒軟體可協助防護電腦不受大多數電腦病毒侵襲

## ➤ 防毒軟體的功能

1. 偵測電腦病毒
2. 系統掃描
3. 處理中毒檔案（刪除、隔離、修復）

## ➤ 病毒碼更新

1. 電腦病毒層出不窮、手法經常翻新、型態不斷改變，需經常更新病毒碼以得到最佳的防護效果

# 個人電腦的資訊安全(9/10)

## ➤ 作業系統的更新

### 1. 系統安全漏洞

1. 發生原因—系統程式開發之疏失
2. 造成影響—在被駭客發現後利用於入侵他人電腦

### 2. 使用Windows Updates

1. 由網路自動下載修補程式並安裝
2. 可修補Windows系統之安全漏洞
3. 可設定排程定期自動查看是否有可下載安裝之修補與更新

# 個人電腦的資訊安全(10/10)

## ➤ 妥適設定政府組態基準(GCB)

1. 依行政院資訊安全處106年7月12日院臺護字第1060180766號函辦理。
2. 教育部106年7月27日函文(院臺教資(四)字第1060101117號函)各直轄市及縣市教育網路中心及臺灣學術網路區域網路中心配合辦理。
3. 政府組態基準(Government Configuration Baseline, 簡稱GCB)目的在於規範資通訊終端設備(如：個人電腦)的一致性安全設定(如：密碼長度、更新期限等)，以降低資通訊終端設備成為駭客入侵管道，進而引發資安事件之疑慮。
4. 行政院於資安稽核時要求設定的GCB項目請參考行政院技服網站政府組態基準(GCB)說明文件(<https://www.nccst.nat.gov.tw/GCB?lang=zh>)相關文件。

---

# 簡報完畢

