電腦安全與個人資料保護防身術

第一篇：《電子郵件安全防護篇》

(一)郵件軟體設定

- 電子郵件軟體應設定為「關閉預覽郵件」。
- 電子郵件軟體以「純文字模式」開啟郵件。
- 電子郵件軟體非必要不設自動回覆。
- 轉寄大量收件者的郵件時，使用「密件副本」 。

駭客隨機測試寄送惡意郵件過程中，若使用者設定自動回覆功能，駭客將會蒐集有效之電子郵件信箱，以進一步騷擾使用者，所以電子郵件軟體不應設定自動回覆功能。

(二)郵件軟體使用技巧

防止社交工程（如網路釣魚）資安事件，請審慎處理電子郵件：

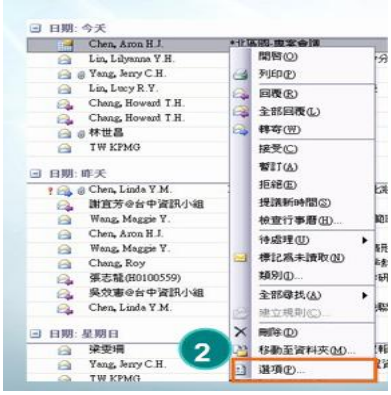
- 瞭解組織傳送郵件規定，不隨意開啟及轉寄與業務無關之電子郵件及網站，避免導致他人中毒。
- 不隨意開啟郵件，如發現不明來源或疑似網路釣魚之郵件應直接刪除。
- 注意陌生寄件者，懷疑信件來源或可疑信件，先透過電話或電子郵件與寄件者確認真偽，或通報學校資訊部門查證。
- 不隨意點選或下載郵件內之連結與附件檔案。
- 不隨意洩露個人 Email 資料。

How to do (1): Outlook 上判斷郵件真偽

步驟 1： 在郵件上按右鍵。

步驟 2： 點選「選項」。

步驟 3： 在下方的欄位中，尋找「From：」。確認 From 之後所標示的位址為自己所知的正常電子郵件來源。

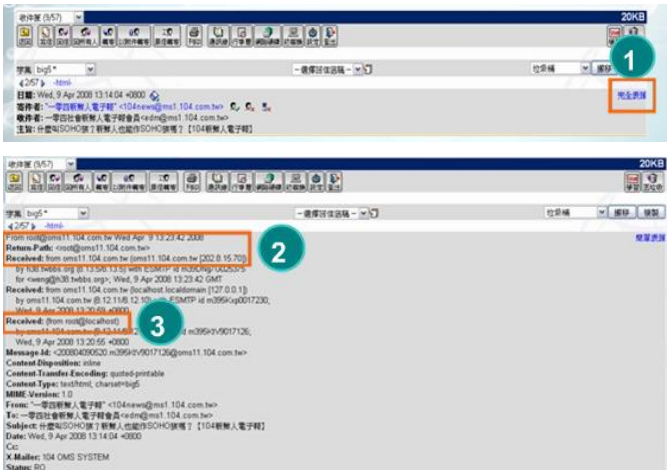


How to do (2):判斷 Webmail 郵件來源真偽

1、點選「完全表頭」，了解 Email 往來完整訊息

2、觀察「Return Path」

3、觀察「Received」

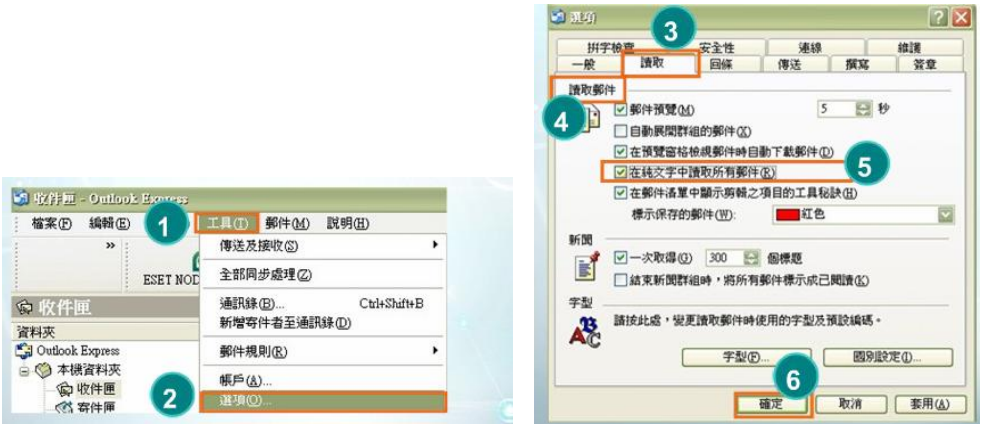


How to do (3):Outlook 關閉郵件預覽

How to do (4):Outlooke Express 關閉郵件預覽

How to do (5):Outlook 以純文字開啟

How to do (6):Outlook Express 以純文字開啟



第二篇：《電子病毒與惡意程式防護篇》

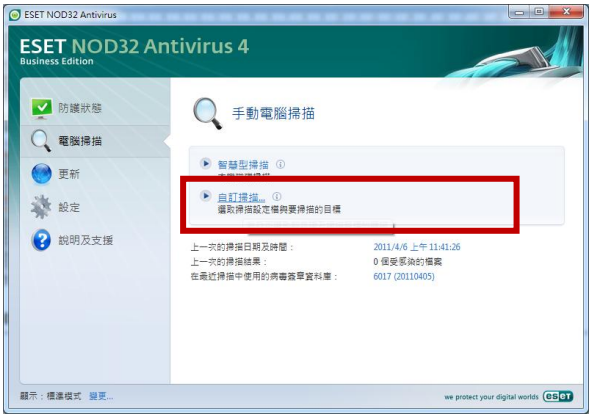
電腦病毒是一種故意設計來干擾電腦運作的程式，常見的干擾行為有破壞電腦檔案、重新格式化硬碟、使電腦效能變慢、上網時瀏覽器不斷打開新視窗，直到電腦資源被耗盡為止等。病毒的傳染途徑包括電子郵件、電腦遊戲，及任何從網路下載的檔案等。

- 安裝防毒軟體，並且定期更新病毒碼。

間諜軟體和病毒相似，會毫無預警地將您的資訊透過網路傳送到特定對象。間諜軟體常伴隨網路免費下載的程式軟體，或點對點音樂檔案交換等管道，入侵您的電腦系統，這不但侵犯個人隱私權也是資安的一大威脅。

- 下載免費或共享軟體前，須仔細閱讀和軟體有關的所有訊息。
- 避免透過點對點傳輸軟體(P2P) 或其他管道下載來路不明的軟體。
- 安裝防毒軟體，並且定期更新病毒碼。

How to do(1)：使用 NOD32 進行電腦掃描

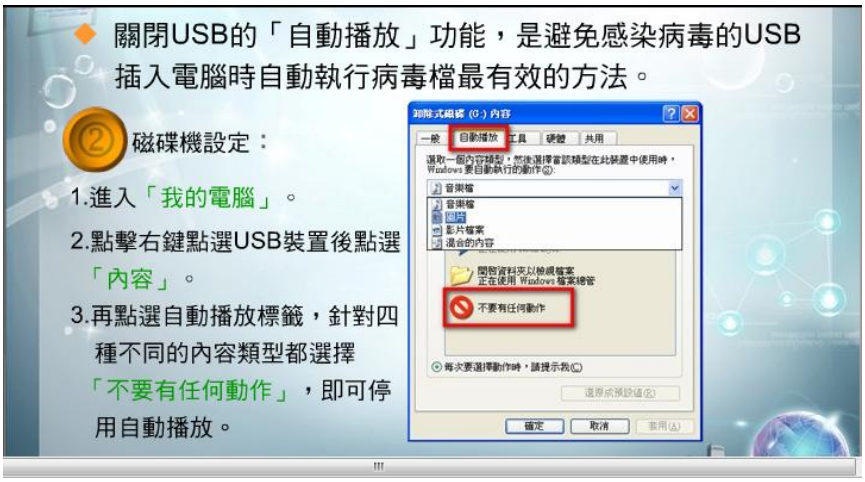


「電腦掃描」/「自訂掃描…」

How to do(2)：關閉 USB 自動執行

方法一：插入 USB 隨身碟時，按住「**Shift** 鍵」不放。

方法二：「我的電腦」/選「USB 裝置」，按右鍵/「內容」/「**自動播放**」



針對四個不同類型的檔，都要選擇「不要有任何動作」

第三篇：《網路個人資料隱私防護篇》

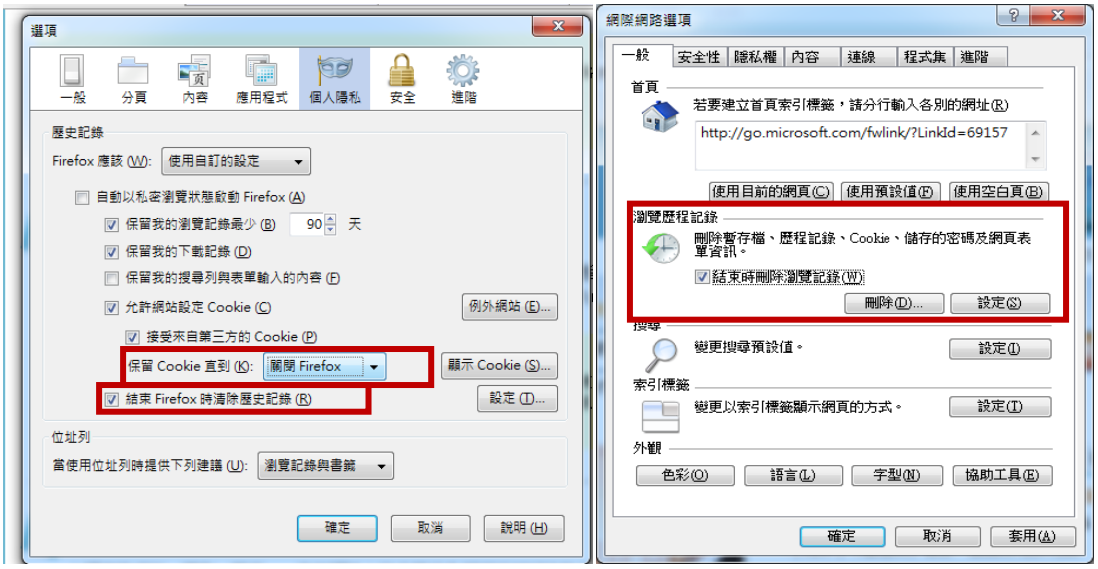
(一)網路紀錄 (cookie)

cookie 是存在瀏覽器中的小型文字檔，記錄使用者瀏覽網頁的資訊、帳號與密碼。當使用者下次再度使用瀏覽器時，電腦能自動顯示最近使用過的網頁，使用者也無需重新輸入帳號與密碼。

- cookie 紀錄重要的個人資料與網路使用習慣，應隨手刪除電腦裡的 cookie 紀錄。
- 詳讀每個網站的隱私權政策，尤其是 cookie 所蒐集的使用者資訊用途，以避免個人資料被濫用。

How to do (1): Firefox – 個人隱私 cookie 設定

Firefox~「工具」/「選項」/「**個人隱私**」/



How to do (2): IE 瀏覽歷程記錄

IE~「工具」/「網際網路選項」/「一般」/「**瀏覽歷程記錄**」

(二) 公用存取

使用圖書館、公司、網咖、機場等地點的公用電腦，或甚至使用室友、朋友電腦時，必須注意所輸入的各種資料是否在這些電腦「留底」，而有資料外洩或遭有心人士利用的風險。

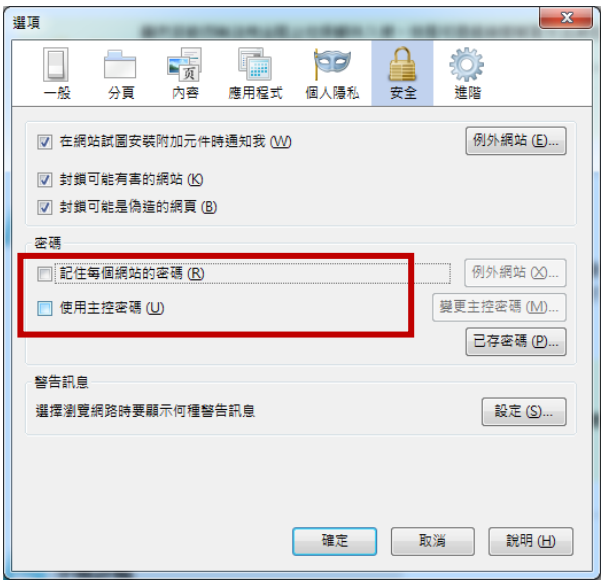
使用公用電腦的守則：

- 使用時留意身旁的人，以免他們看到您的個人資料。

- 絕不勾選網路瀏覽器的「記住密碼」選項。
- 儘量不在公用電腦中輸入敏感性高的資訊。
- 結束使用時，應關閉網路瀏覽器，若有「登入」帳號（如電子郵件），應完成「登出」後，再關閉瀏覽器。離開前，也應登出系統或將電腦關機。
- 若經常使用公用電腦，更換密碼的頻率要更高。

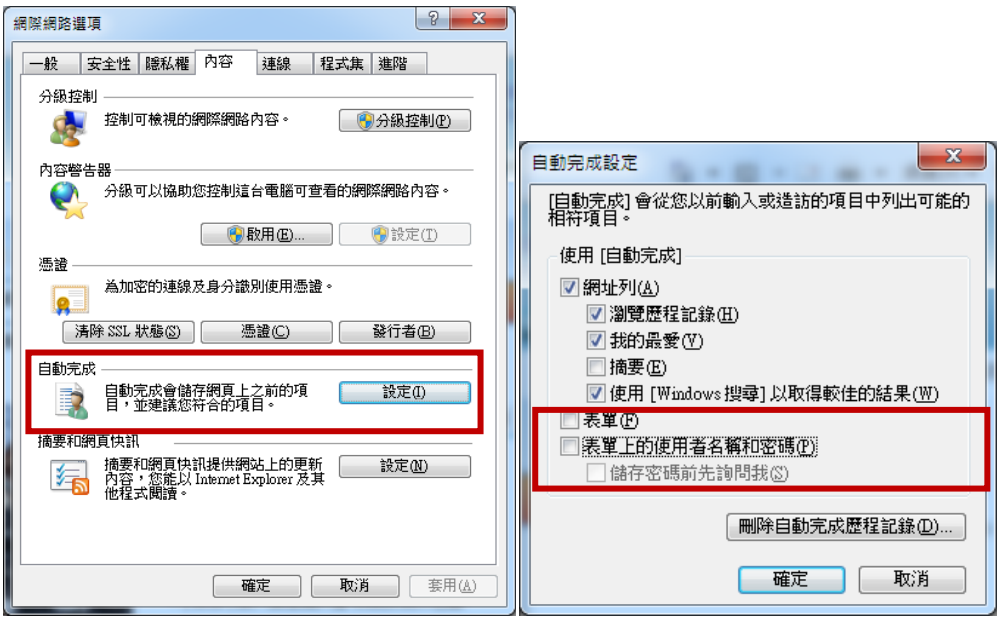
How to do (1) : Firefox 不要自動記住我的密碼

Firefox~ 「工具」/「選項」/「安全」/「密碼」



How to do (2): IE 不要自動記住我的密碼

IE~「工具」/「網際網路選項」/「內容」/自動完成 /「設定」



《第四篇》個資保護七大妙招

1. 電腦開機設密碼 每三個月要更新 – 記得幫自己的電腦和家用電腦設定開機密碼，保護裡面的資料不會被其他人閱讀，並且，每隔三個月要定期更新密碼，才能確實達到對電腦的安全保護。
2. 英文數字混符號 密碼強度才足夠 – 當我們在設定電腦開機密碼或是個人信箱密碼時，請記得使用「大寫英文字母」加上「數字」再加上「特殊符號」混合而成的密碼，並且，密碼長度最好超過 8 碼，才能確保密碼不至於被不肖人士破解。
3. 公用電腦請小心 帳號密碼不留存 – 出門在外使用公用電腦時，千萬要避免操作需要鍵入個人帳號密碼的網頁，如果不得已需要開啟這些平台，一定要確認帳號密碼沒有被網頁自動記錄下來，還有，離開電腦前記得登出自己的帳號喔！
4. 電腦送修先備份 原始資料清乾淨 – 如果電腦必須進行修理，請先將裡面的原始資料另外備份，並將資料全數刪除後，再送交工程人員進行修理，以避免重要的個人資料外洩。
5. 填寫個資請留意 隱私條款詳細讀 – 如果因為申請個人信箱、參與網路活動或是加入網站會員必須填寫個人資料時，千萬要詳細閱讀網站中的隱私權聲明，確保該網站設置有防火牆和防毒系統來保護我們的資料，以及只有網站授權的工作人員才能閱讀我們的資料。
6. 個資換獎危險多 小心辨識不貪心 –如果在網路上或是現實生活中，遇到提供個人資料就可以換取獎品的活動或是機會，記得請家長協助判斷，因為這些都有可能是詐取個資的手段。
7. 網路互動高警覺 個人資料勿坦白 –當我們在網路上發言或是與網友互動時，千萬不要透露太多的私人資料，例如姓名、學校、電話號碼、家裡地址，以及身分證號碼等等，因為我們不知道這些資料會不會被有心人士移做非法的用途。

資料來源：

教育部全民資安素養自我評量網站《資安手冊》

教育部《教育機構資訊安全認知教育訓練線上教材》