國立馬公高級中學個人電腦資訊安全注意事項

108.06.16更新

說明：我國資通安全法於 108 年正式施行，本校資通安全維護計畫亦於 108 年11 月26 日會議通過， 依規定，資訊及資通設備之使用，須遵守相關規範，摘錄如下。

(一)每人每年接受 3 小時以上之一般資通安全教S育訓練。

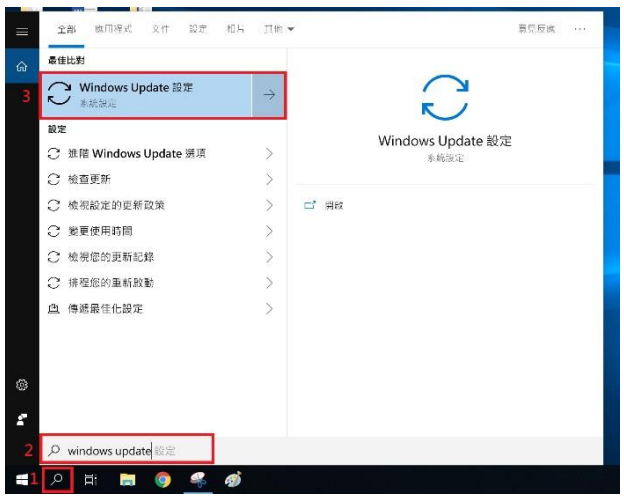
(二)電腦使用安全管理

1. 電腦應隨時配合更新作業系統、應用程式漏洞修補程式及防毒病毒碼等，以避免惡意軟體利用系統或軟體漏洞　進行攻擊。

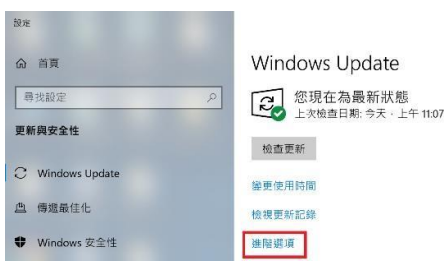
(1) 定期更新並及時修補作業系統漏洞、應用程式。

【方法】Windows Update(以 Windows10 為例)

- 點選電腦桌面底下工具列 圖示　輸入「Windows Update」　選擇搜尋到的「Windows Update 設定」選項　點選「檢查更新」查看電腦目前更新狀態。



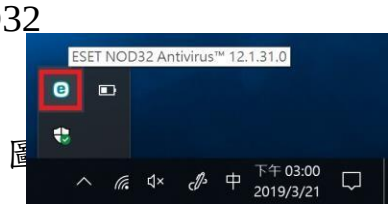
- 選擇「進階選項」　確認「更新選項」內容皆為開啟之狀態。



(2) 安裝防毒軟體並更新病毒碼。

【方法】本校之防毒軟體為ESET NOD32

- 檢查右下角工具列中是否有　圖示，確定防毒軟體於開機後正常啟動。



- 對  圖示按右鍵　選擇「檢查更新...」

  再點選視窗右下角「檢查更新」確認是否更新至最新的防毒引擎與病毒碼，病毒碼每 1 至 2 天會更新。

2. 電腦若超過 15 分鐘不使用時，應立即登出或啟動螢幕保護功能並取出自然人憑證。

【方法】滑鼠在桌面按右鍵，選「個人化」　「螢幕保護裝置」，等候時間為「15 分鐘以下」，並勾選「繼續執行後，顯示登入畫面」，即可以登入密碼保護。

3. 依據現行個人資料保護法規定，國民身分證統一編號屬個人資料，為減少使用者個人資料曝露範圍，並強化資　訊系統帳號及密碼之安全性，資訊系統不應使用身分證統一編號做為帳號名稱，亦不可使用弱密碼做為使用者　密碼，並請遵守下列密碼複雜原則：

(1) 長度 8 碼(含)以上，建議至少包含英文大寫、英文小寫、數字、符號任 3 種。

(2) 複雜度不得與前三次設定之密碼重覆。

(3) 使用者每 90 天應更換一次密碼。

4. 禁止共用帳號及使用瀏覽器記住帳號、密碼之功能。

5. 下班時應關閉電腦及螢幕電源。

(三)通訊安全管理

1. 非必要請勿開啟網路芳鄰或共享資料夾。

2. 本校不開放遠距工作。

(四)電子郵件安全管理

1. 應使用純文字模式瀏覽，避免讀取來歷不明或含有巨集檔案之郵件，郵件如有夾帶附件，請先掃描是否存有惡　意軟體。

2. 不得傳送機密性或敏感性之資料，如有業務需求者應進行加密或其他之防護措施。

3. 使用者不得利用電子郵件服務從事侵害他人權益或違法之行為。

4. 防止電子郵件社交工程(網路釣魚)資安事件，請關閉郵件預覽功能，開啟郵件前審慎查證下列資訊：

(1) 寄件來源、郵件主旨　(2)是否業務或工作需要(3)郵件內異常網址連結判斷　(4)附加檔案之觀察

5. 應配合上級機關辦理電子郵件社交工程演練。

(五)防範惡意軟體措施

1. 使用外接式儲存媒體(磁碟片、光碟片、USB 隨身碟、隨身硬碟...等)前必須開啟

防寫裝置並進行病毒掃瞄。

2. 請勿私自連結使用已知或有嫌疑惡意之網站。

(六)資料儲存與備份管理

1. 勿將重要資料儲存於桌面，並將「我的文件」資料夾及其他儲存重要資料之資料夾設置於D 磁碟中，本校電腦均設有 DVD 燒錄機，若有重要資料，請務必自行做好定時與備份工作，必要時得進行異地備份。

2. 資訊設備之歸還應確保個人資料已備份並抹除。

3. 本校公用電腦固定安排於暑假進行維護整理，敬請務必自行於六月底前備份完畢。

(七)加密管理

1. 機密資訊於儲存或傳輸時應進行加密。

(八)軟體使用

1. 禁止安裝及使用未經授權之軟體，並遵守智慧財產權相關規定。

2. 不下載及安裝來源不明的軟體，以防惡意程式入侵電腦，並請注意做好定時與異地備份，以防發生勒索病毒資 安事件。

3. 禁止私自安裝點對點（Peer to Peer, P2P）軟體，例如：Foxy、iMesh、 eDonkey、BT、ClubBox、GoGoBox
等，以防惡意程式入侵電腦。

(九)辦公室區域之實體與環境安全

1. 應考量採用辦公桌面的淨空政策，以減少文件及可移除式媒體等遭未被授權的人員取用、遺失或是被破壞的機 會。

2. 文件及可移除式媒體在不使用或不上班時，應存放在櫃子內。

3. 機密性及敏感性資訊，不使用或下班時應該上鎖。

4. 存放機密資訊或具處理機密資訊之通訊錄，不宜讓未經授權者輕易取得。

5. 資訊或資通業務相關設備，未經管理人授權，不得被帶離辦公室。

本注意事項，敬請同仁配合！謝謝～～～