鼎金國民中學教師資訊安全宣導

各位教師:

以下十大資訊安全基本原則概念宣導，請各位同仁參閱，共同合作以提高校園網路使用安全保障

- 一、牢而不破的密碼設定:　良好的使用習慣
  - 不告訴別人密碼，包括男女朋友、職務代理人、上司等。
  - 若懷疑有人可能知道你的密碼時，即刻更改。
  - 不設定過於複雜難記的密碼。
  - 不寫下密碼　。
  - 定期更換密碼。
- 定期更新密碼
  - 為確保密碼的機密性，使用者應定期更新密碼，減少密碼外流的機率。
  - 當單位內部有人員異動，應立即進行相關密碼與使用代號更新。
    - 至少每三個月更新一次密碼
    - 將密碼存放於高安全性的地方
    - 刪除無效的使用者帳號
- 設定優質密碼
  - 設定優質的密碼（不容易被猜中的密碼）
    保護各個電腦系統是非常重要的。
    為減少密碼遭受駭客破解所造成損失，電腦管理者也需要一套程序來確保密碼的正常運作。
  - 設定優質密碼的秘訣如下：
- 設定至少 8 個字元的密碼
- 密碼設定建議字元至少需為 8 個字元的字串。
- 為提高密碼使用的安全性，設定 8 個以上字元的密碼字串，並且定期更新密碼，可提高密碼的安全性。
- 避免使用重複的字母或數字，如 aaa1122, 555iii99。
- 使用數字、字母、符號混合穿插的密碼字串。
  - 為增加密碼被破解的難度，應避免使用簡單且他人容易取得的資料為個人密碼（姓名、電話、生日、電子信箱網址等）。
  - 建議以大小寫字母、數字、及符號（＃％＄@…）混合方式設定密碼。
- 定期更新密碼
  - 為確保密碼的機密性，使用者應定期更新密碼，減少密碼外流的機率。
  - 當單位內部有人員異動，應立即進行相關密碼與使用代號更新。
    - 至少每三個月更新一次密碼
    - 將密碼存放於高安全性的地方
    - 刪除無效的使用者帳號
- 避免重複使用已使用過的密碼
- 避免使用簡單且字典查得到的單字或學校名稱縮寫
- 檢測密碼強度：
  - http://www.refly.net/passwordchecker
  - http://www.microsoft.com/taiwan/athome/security/privacy/password_checker.mspx

二、遠離網路釣魚犯罪陷阱與騙局

- 網路犯罪集團常利用電子郵件或網頁進行網路釣魚行為，使用者須注意任何信函以及網址正確性，先從字面分辨與確認信函的正確性，以提高警覺度。
- 防範訣竅：
    - 不回應任何來自不明單位於電子信件中要求提供個人隱私安全相關資訊，這些資訊包括使用者名稱、密碼、帳號。
    - 不點選來路不明的電子郵件中所載之網頁連結。
    - 不利用校園網路轉寄垃圾信函。
    - 點選網頁連結前請一定要仔細辨認。

三、確保工作領域的私密

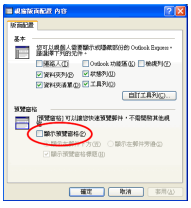
- 員工經常會把機密性資料文件、備忘紙、以及記載個人相關資訊等文件，隨意放置於桌上。
- 或者將資料進行完善的分類，並且儲存在電腦桌面上，這些動作都很容易導致資料的外洩。
- 防範訣竅：
    - 當離開個人座位時，啟動鎖定功能(視窗鍵+L)或設定螢幕保護程式，並設定關閉螢幕保護程式的密碼。
    - 教育員工提高警覺，不在桌面上放置重要文件，或使用可上鎖的抽屜等設備保管機密文件。
    - 行政共用資料夾 R 槽，絕不可放個資相關檔案，亦不可公開於網站

四、確保網路瀏覽器使用

- 許多微軟 IE 使用者將瀏覽器安全控制程度設定降低以方便網頁讀取，但這很可能讓網路瀏覽器成為惡意程式侵入電腦的管道。
- 當使用者瀏覽具有惡意程式的網頁時，可能因為安全控制程度設定值不高，自動下載惡意程式使電腦造成損害。
- 防範訣竅：
    - 建議將讀取網頁瀏覽器安全層級設定為中安全性以上。
- 防範訣竅：
    - 對於經常使用且可信任的網站，可預先於工具列中設定該網址為可信任，以避免瀏覽器在高安全層級設定下，導致網頁無法正常讀取之困擾。
    - 改用其它較安全的瀏覽器軟體，如 FireFox…等。

五、正確的使用電子郵件

- 電腦病毒傳播最經常的途徑為電子郵件，不隨意開啟電子郵件附夾檔案為資安保全基本要件。
- 防範訣竅：
    - 關閉郵件預覽功能。
    - 檢視→版面配置→



- 防範訣竅：
    - 除非使用者相當確定信件來源與信件夾帶的附件內容為何，否則決不輕易開啟或執行電子信件裡的附件檔案。
    - 安裝防毒軟體。
- 除了上述的防範訣竅，對於電子郵件的正確使用與資訊安全、權益維護，還包括下列幾點：
    - 不要將電子郵件密碼告知任何人，即使對方是系統管理者。
    - 不要將電子郵件帳號轉借他人使用。
    - 不要使用電子郵件傳輸任何不當資訊，包括不法、暴力、色情、違法交易、侵犯隱私或威脅他人的資料。

- 不要轉寄不明網路謠言及發送廣告信。
- 避免在電子郵件夾帶大容量檔案，以免造成收件人收信時間冗長的困擾。
- 轉寄或回覆郵件時，勿隨意修改作者原始文字。
- 郵件中如含有他人之個人隱私資訊，在轉寄時應先取得同意。

六、確認防毒軟體隨時運作

- 防毒軟體的偵測與防範功能只有在該軟體有在運作、且有時常更新病毒碼情形下，才會產生效用。
- 防範訣竅：
  - 不關閉、不刪除防毒軟體。
  - 隨時注意防毒軟體的病毒碼是在最新的狀態。
  - 定期執行掃毒。

七、勿隨意安裝未經許可的電腦軟體

- 網路上有許多免費分享的實用軟體或遊戲，但通常提供企業使用的軟體並非永久免費的。
- 任意下載、安裝網路上的免費軟體、或來路不明的軟體，也是感染電腦病毒、間諜軟體與特洛依木馬程式的主要途徑。
- 某些合法軟體因為不明軟體的使用產生衝突情況，也可能因此造成電腦系統部故障。
- 防範訣竅：
- 絕對不下載、安裝未經許可的軟體

八、謹慎使用即時通訊軟體

- 即時通訊軟體（如 LINE、Wechat…等）雖然是快速且方便的網路溝通工具，但也有可能成為電腦病毒傳遞途徑，也可能遭受其它惡意程式與網路釣魚的攻擊，使用即時通訊系統時必須小心謹慎。
- 正確的運用方法：
  - 登入密碼最好不要用「儲存密碼」記錄於系統內。
  - 不任意傳遞與分享單位重要資訊或檔案。
  - 不任意接收來路不明之分享檔案和連結。
  - 使用者必須秉持以公事使用之目的使用即時訊息。
  - 隨時更新使用端程式。

九、確保軟體在更新狀態

- 當軟體被使用一段時間後，通常會出現一些小問題或安全漏洞，這些漏洞也是駭客容易利用的弱點，**零時差攻擊**即目前駭客最喜歡利用的手法。
- 因此信譽好的軟體商通常會設計更新或修補程式來修正這些問題。
- 防範訣竅：
  - 檢查以下重要應用程式或軟體是否為最新版本：
    - 作業系統(Windows XP 或 2000、Mac、Linux…等)
    - 網頁瀏覽程式(IE、FireFox…等)
    - 辦公室應用軟體(Office、Adobe PDF…等)
    - 電子郵件收發軟體(如 outlook、outlook express…等)
  - 大部分的軟體都會提供一項「自動更新」功能，啟動自動更新功能為最方便也最迅速的一種定時更新方法。

十、正確使用可攜式媒體

- 自動播放不等於自動執行。

- USB 病毒利用自動播放的特性去誘導出自動執行的動作，進而去執行(開啟)惡意的程式。
- 有效避免自動執行的方法：
- 自動播放不等於自動執行。
- USB 病毒利用自動播放的特性去誘導出自動執行的動作，進而去執行(開啟)惡意的程式。
- 有效避免自動執行的方法：
- 檔案總管操作法
    - 開始→我的電腦(按右鍵)→檔案總管

或是利用快捷鍵：視窗鍵 + E

    - 點選左邊窗格 USB 媒體→開啟檔案
- 電腦管理服務設定法
    - 開始→我的電腦(按右鍵)→管理→電腦管理→服務及應用程式→服務
    - 停用 Shell Hardware Detection 服務
- 新增使用者 Everyone。
- 設定使用者 Everyone 的完全控制權限為「拒絕」，選取套用/確定後離開。
- 參考資料來源: www.nutn.edu.tw/gac600/class/**資訊安全**基本素養教育訓練**.ppt**