

網路安全與保護學習單

班級 _____ 座號 _____ 姓名 _____

一、惡意程式的問題

1. 認識惡意程式：

- (1) _____ (virus)：具有破壞性或惡作劇性質的電腦程式。
- (2) _____ (Trojan horse)：「依附」在電腦檔案中的惡意軟體，以竊取他人的私密資料為目的。
- (3) _____ (worm)：會不斷地大量自我複製，並藉由網際網路的管道來散播，會造成電腦、網路及郵件伺服器無法正常運作。

2. 惡意程式的防範措施：

- (1) 安裝_____
- (2) 養成良好的電腦使用習慣
 - A、不使用_____
 - B、不任意開啟_____
 - C、避免瀏覽_____
 - D、定期_____

3. 電腦感染惡意程式的補救處理步驟

- (1) 使用_____進行掃毒及解毒的工作
- (2) 若無法解毒，可利用_____上網下載解毒程式
- (3) 關閉_____；若病毒是透過網路傳播，應先_____
- (4) 重新開機，開機時按_____鍵，以_____模式進入 Windows 作業系統
- (5) 使用_____進行解毒

二、駭客入侵的問題

1. 駭客攻擊的手法：

- (1) 入侵網站：竊取資料或篡改網站內容
- (2) _____攻擊：在網頁中植入惡意程式。
- (3) 散布惡意程式：
- (4) _____(DoS)攻擊：藉由發送大量訊息，使網站癱瘓。

- (5) _____(BotNet)：透過網路散布具有遠端遙控功能的惡意程式，並搖控受感染的電腦來濫發垃圾郵件、竊取他人資料。
- (6) _____攻擊：利用軟體本身的安全漏洞進行竊取資料、植入病毒等行為
- (7) _____攻擊法：駭客收集「字典」檔，並透過一一嘗試的破解方式，來找出密碼。可透過圖型驗證碼來防範。
- (8) _____：駭客建立與合法網站極為相似的網頁畫面，誘騙使用者在網站中輸入自己的帳號、密碼、信用卡卡號，以取得使用者的私密資料。

2. 駭客入侵的防範措施：

- (1) 安裝_____
- (2) 養成良好的電腦使用習慣
- A、下載並安裝_____
- B、妥善管理自己的_____，並定期_____
- C、避免使用_____進行_____
- D、登入網站前，確認_____
- E、勿直接點按_____來登入網站
- F、機密資料儲存在_____或_____中

3. 設定及管理密碼的原則

- (1) _____個字元以上
- (2) 使用_____、_____、_____混合
- (3) 避免使用_____（如生日）作為密碼
- (4) 不定期_____，且勿隨意_____
- (5) 勿用「_____」，如："1111"、"1234"、"password"、"abc123"

三、安全資料傳輸層（_____）是保護網路上資料傳輸安全的安全規範。網路購物時，最好選擇網址開頭為_____，表示該網站使用_____安全規範。