投稿類別：資訊類

篇名：

高中職生對惡性程式認知程度探究 — 以高雄市樹德家商爲例

作者：

唐瑋廷。私立樹德家商三年 6 班

郭釗榮。私立樹德家商三年 6 班

吳尙修。私立樹德家商三年 6 班

指導老師：

黃珮華老師

壹●前言

一、研就動機

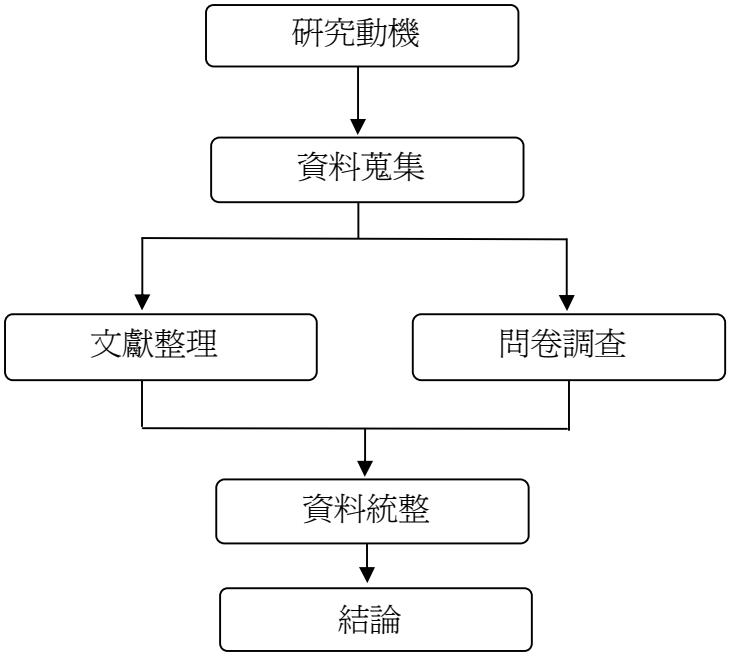
以目前的高中職生而言，週遭有很多人對於電腦中毒當下，近八成會選擇重灌電腦而不了解爲何會中毒，卻一次又一次的重蹈覆轍。因此我們想了解目前的高中職生對惡性程式的知識深淺。

二、研究目的

藉由文獻及問卷統計，探討高中職生使用網路的時間以及對惡性程式各種特性的了解。

三、研究流程

（圖一　本文流程圖）



貳●正文

一、惡性程式定義

Malicious Software 英文簡稱 ”Malware” 惡意程式是一個統稱!病毒,木馬,蠕蟲,間諜程式等等十多種分類和其他一切對電腦有惡意或是有害的程式,我們都統稱爲惡意程式！

二、惡性程式介紹

(一)、惡性程式的種類

1.病毒：電腦病毒會從宿主程式上複製自己，以在不同應用程式或系統間傳播，感染其它使用者的檔案，病毒可能會挾持、破壞使用者的檔案與磁碟。

2.木馬：不會自行複製或感染，但是被啓動後就會執行像開啓後門之類的惡意行爲，讓使用者系統處在無防備的狀態，導致使用者系統被利用或當作跳板，也可能作爲其它攻擊的前導。

3.蠕蟲：會自行複製，但是不會感染其它檔案，蠕蟲會利用系統與網路的漏洞，傳播到網路上的任何一台連接的電腦上，造成網路、系統的癱瘓。

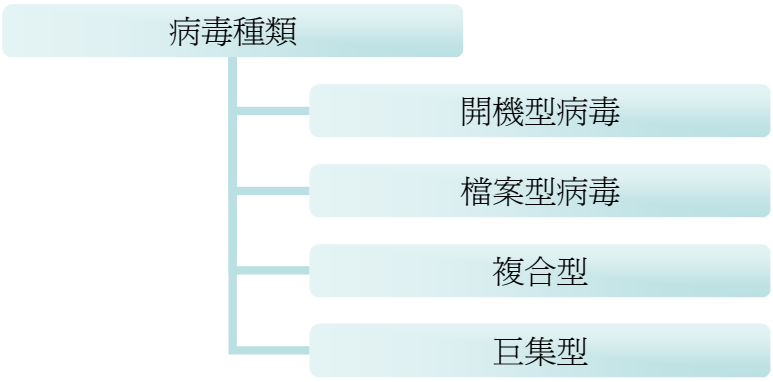
(二)、**解決方式：**

1.如果已經中毒,避免再度使用中毒電腦輸入任何有關帳號跟密碼的欄位！

2.即刻利用其他電腦更改,再重灌 c 槽. d 槽。信件本身是不會附載病毒的，真正具有病毒威脅的是信件所夾帶檔案。

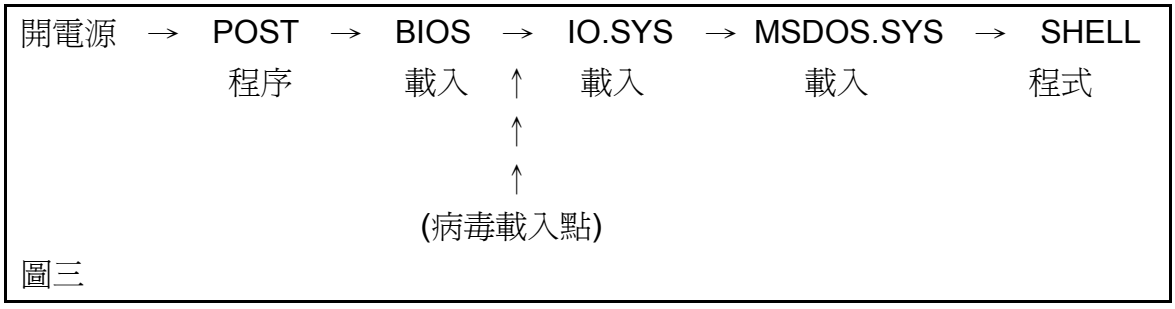
(三)、病毒的種類

（圖二　病毒種類圖）



1、開機型：

所謂開機型的病毒(Boot-type virus) 是界定爲在電腦開機時，搶先作業系統進入記憶體的程式。



圖三

(1).傳統開機型病毒：

純粹的開機型病毒多利用軟碟開機時侵入電腦系統，再伺機感染其他的軟碟或硬碟。

(2).隱形開機型病毒：

Ｃ槽 BRAIN，凡是爲此病毒感染之系統，再行檢查開機區，得到的將是正常的磁區資料，就好像沒有中毒一般，此型病毒較不易爲一般掃毒軟體所查覺，而防毒軟體對於未知的此型病毒，必須具有辨認磁區資料真僞的能力。

2、檔案型：

檔案型的病毒(File-type virus) 是介定爲檔案執行時，在原檔案之前執行的程式。病毒本體寄居於可執行檔案中，當此檔案被執行時，便侵入作業系統取得絕對控制權。

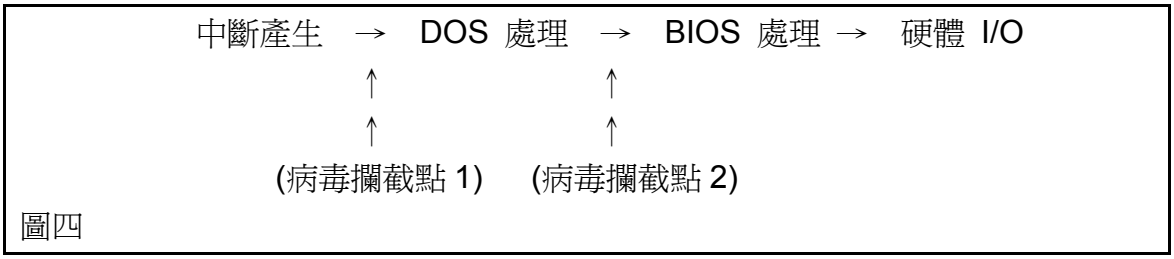
(1).傳統檔案型病毒：

檔案感染型病毒最大的特徵，便是將病毒本身植入檔案，使檔案膨脹，以達到散播、傳染的目的。

(2).隱形檔案型病毒：

有越來越多的跡象顯示，隱形感染可避開許多防毒軟體的偵測。直接植入 DOS 的作業環境中，當外部程式呼叫 DOS 中斷服務時，便同時執行到病毒本身，使得病毒能從容地將受其感染的檔案，粉飾成正常無毒的樣子。

※它可能會有兩種侵入的方式※



圖四

3、複合型：

複合型(Multi-partite) 病毒綜合了開機型及檔案型的特性，以及兩者的感染方式，更加快了病毒程式散播的速度，如國內較常見的 MacGyver 2.0 就屬這一類型（通常也是病毒作者用來提升技術而使用）。

4、巨集型《文件導向式的病毒染》:

所謂的「巨集」，是用來記錄在應用程式中所進行的一連串操作，這些操作往往和特殊的按鍵設定關連，只要按下這些按鍵，就可以自動執行原先設定的一連串指令。

三、木馬與駭客間防範惡性程式的入侵

(一)、木馬的定義

1.特洛依木馬程式介紹：

特洛伊木馬程式(Trojan Horse)是一種惡性程式而非病毒，和病毒(Virus)最大的不同是：特洛伊木馬通常不會自我複製，大多用來竊取電腦密碼以及私密資料。。

2.特洛伊木馬的特徵：

(1)不需要本身的使用者准許就可獲得電腦的使用權。
(2)程式體積十分微小，執行時不會佔用太多資源。
(3)執行時很難停止它的活動。
(4)執行時不會在系統中顯示出來。
(5)一次執行後，就會自動登錄在系統啓動區，之後每次在 Windows 載入時自動執行。
(6)一次執行後，就會自動變更檔名，甚至隱形。
(7)一次執行後，會自動複製到其他資料夾中。
(8)做到連本身使用者都無法執行的動作。

※防範：

感染之後若要除去，除了利用防毒軟體外還可以透過刪除所有暫存資料夾、以反間諜軟體掃描系統註冊檔等方式去除。真正能夠避免感染的方法還是培養良好習慣、不要下載來源不明或看起來可疑的程式與檔案。

※.預防方法：

(1) 不要執行任何來歷不明的軟體
(2) 不要隨意打開郵件附件
(3) 重新選擇新的用戶端軟體
(4) 將檔案總管設定成"始終顯示副檔名"
(5) 儘量少用"共用文件夾"
(6) 經常更新系統

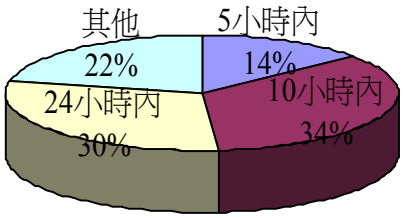
(三)、駭客入侵五個常用手段

1.建立模擬環境，進行模擬攻擊，測試對方可能的反應。
2.利用適當的工具進行掃瞄。
3.實施攻擊。
4.常用工具介紹。
5.常用工具：

(1) 口令入侵
(2) 特洛依木馬(trojan horse)
(3) 網路嗅探器(Sniffer)
(4) 破壞系統

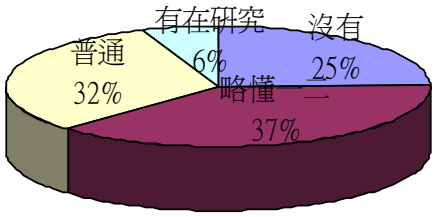
四、對於惡性程式與防範的問卷

1.一週內使用電腦的時數?



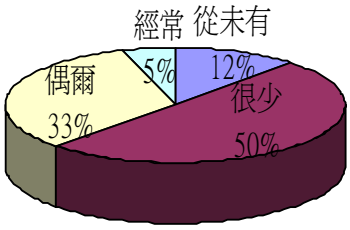
由調查顯示，高職生在一週內使用電腦的時數爲 10 小時內者爲最多。

2.你對惡性程式的徵兆認知?



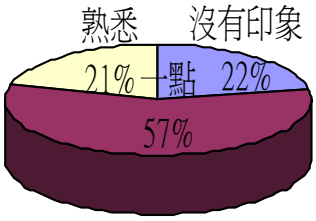
由調查顯示，高職生對惡性程式的徵兆認知略懂者佔37%爲最多，可見基本上高中職生對惡性程式都有一定的了解。

3.你的電腦常常中毒嗎?



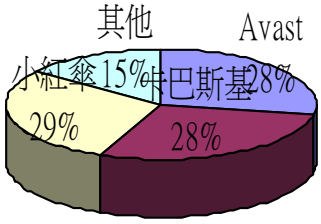
由圖可知道，個人電腦很少中毒的現象者佔 50%，也表示高職生對於防止電腦病毒入侵有一定程度上的瞭解，也有可能中了惡性程式卻不自知。

4. 你對於惡性網址的特徵熟悉嗎?



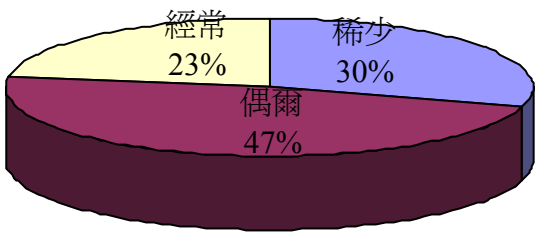
由研究可知，對於惡性網址有一點印象者佔 57%，可見高中職生對惡性網址是會去留意的。

5. 你最常使用的電腦防毒軟體有哪些?



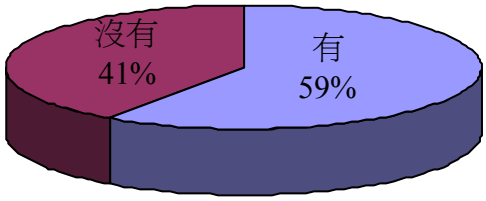
大部份高職生都使用 Avast、小紅傘、卡巴斯基這三種防毒軟體比較普遍。

6. 有收過通訊軟體的垃圾網址嗎?



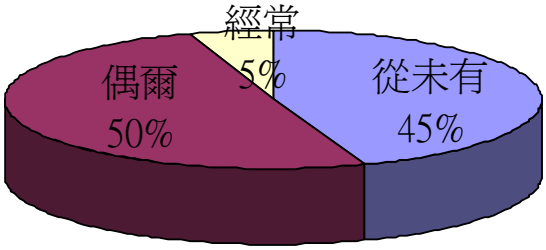
由此可見，有使用通訊軟體的高中職生幾乎都接收過垃圾網址的散播。

7. 家裡電腦曾有過惡意程式的侵害嗎?



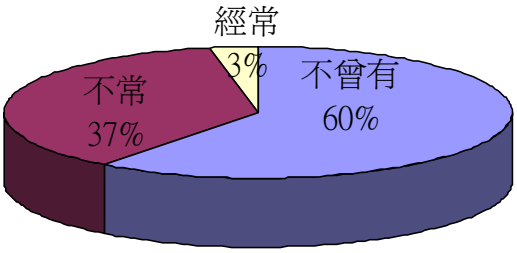
由此可知，學生使用網路有將近六成使用者遭受惡性程式的侵擾。

8. 請問你的帳號密碼有經常被盜用嗎?



由圖可知，廣泛使用網路的高中職生有進一半以上的人都曾遭受盜用。

9. 你曾經有過帳號無故被凍結嗎?



經過統計後，有關線上程式有辦理帳密的使用者，有六成不曾有過帳號凍結的情形。

參●結論

對於高職生對惡性程式認知程度探究，由**問卷研究**顯示，高職生在一週內使用電腦的時數爲 **10 小時內**者爲最多。對惡性程式的徵兆認知**略懂**者佔 37%最多，可見基本上高中職生對惡性程式都有一定的了解。

大部分同學表示，個人電腦**很少**中毒的現象者佔 50%，可見高職生對於防止電腦病毒入侵有一定程度上的瞭解，也有可能中了惡性程式卻不自知。對於惡性網址有一點概念者佔 57%，可見高中職生對惡性網址是會去留意的。

大部份高職生都使用 **Avast、小紅傘、卡巴斯基**這三種防毒軟體**比較普遍**。有使用通訊軟體的高中職生幾乎都接收過垃圾網址的散播。學生使用網路有將近**六成**使用者遭受惡性程式的侵擾。廣泛使用網路的高中職生有將近一半以上的人都曾

遭受盜用。有關線上程式有辦理帳密的使用者，有 6 成不曾有過帳號凍結的情形。

肆●引註資料：

●談論電腦病毒：http://www.csie.ntu.edu.tw/main.php

●CRETIXSecurityArticles：http://www.hacker.org.tw/

●韓筱卿、王建鋒、鐘瑋(2007)。**電腦病毒技術分析與防範**。台北：松崗