

10 駭客不上身 - 病毒防護



【學習重點】

1. 能養成正確使用習慣，避免電腦病毒的危害。
2. 能不隨意下載及安裝不明的程式。
3. 能懂得如何管理與保護自己的檔案。

1 一觸即發

「流暢的科技應用力」是21世紀學生的關鍵能力之一，現代的國小學生已經藉由電腦資訊課程，學會了如何使用網路搜尋、文書處理和簡報製作的基本技巧，也開始應用電腦來製作學科報告以及各項作業，而這也意味著同學們對於資訊科技的依賴會愈來愈深。

許多同學會選擇利用隨身碟、網路硬碟…等，來儲存與管理自己的重要資料，因此，如何妥善保存或保護好重要資料就成為新一代「數位原住民」的必修課題；因為，不良的科技使用習慣，恐怕會造成電腦中毒、個資外洩甚至帶來無法預知的後果以及慘痛的代價…。



一、隨身碟中毒事件

(一) 故事情節

假日，社區圖書館的一角，米迪、沃德正和幾個小組同學們一起，小聲地討論著自然科的「臺灣瀕臨絕種的動物」專題報告作業，他們這一組選擇的是「黑長尾雉」；米迪是小組長，負責主持討論以及上臺進行報告，沃德則自告奮勇要將大家討論後的報告整理成文件，其他同學則負責查資料、影印、製作簡報…等。

小組的同學們都非常認真，大家興高采烈、七嘴八舌的討論完畢之後，沃德拿出自己準備好的隨身碟，將剛才整理的檔案儲存起來，以便帶回家後繼續修改。隔天，小組同學們利用午休時間聚集在電腦教室，準備繼續完成最後的專題報告與簡報。



米迪：「沃德，把昨天的檔案打開來吧！我們繼續討論，一起來把最後的簡報完成。」

沃德：「OK, No problem，包在我身上。」沃德帥氣地拿出隨身碟，並將它插入學校電腦的USB槽準備大顯身手，卻突然驚叫了起來：

「咦！怎麼搞的，我的隨身碟讀不到資料了？」

「什麼！電腦竟然要我進行格式化才能使用！」

這下糟糕了，大家圍過來，你一言我一語的卻沒有一個人知道接下來應該怎麼做才好。

「那，我存在裡面的檔案怎麼辦？」

沃德望著電腦大聲哀嚎！兩手不停抓著頭髮，急得滿頭大汗，眼淚已經快要掉下來了。

「我的暑假作業，還有我最心愛的電腦遊戲都存在裡面，這下完蛋了啦！？」



（二）問題討論

1. 你覺得沃德的隨身碟發生了什麼事？
2. 如果是你遇到這種狀況，你會如何處理？
3. 如何才能避免這樣的情形發生？



二、臉書購物社團事件

（一）故事情節

上完電腦課，佩琪和伊妹還在座位上低聲聊天，好像在商量著什麼祕密大事，好奇心重的米迪看見了就走過來湊熱鬧。

米迪：「妳們兩個下了課還不走，是在偷偷說誰的壞話啊？」

伊妹：「哪有！我們只是在聊，最近我們的臉書帳號都被沃德加入一些莫名其妙的購物社團的事；雖然上面的『圓仔小書包』和『圓仔抱枕』確實很可愛啦，但不知道他到底在想什麼？讓人覺得很困擾，又不知道要怎麼跟他說…」

佩琪：「對啊～而且上面標的價格都很可疑…」

米迪：「啊～小心點，這些很多都是詐騙的網站！原來你們跟我一樣也是受害者，我也正想找他問清楚，不如我們一起去找他理論吧！」





帳號盜用

於是，佩琪和伊妹就跟在米迪後面，此時，沃德已經將電腦關好機，正準備離開電腦教室，米迪從背後大聲地叫住他：「沃德，等一下，我們有事情要問你。」

沃德：「什麼事？」

米迪：「你最近為什麼一直把我們加入一些莫名其妙的臉書購物社團？這種事情，應該要先問過我們的意願吧？」

沃德：「你在胡說些什麼啊？我什麼時候把你們加入社團了？根本就沒有這回事好不好！」

米迪：「喔…還不承認？證人可不只我一個，不信你問她們…」

佩琪和伊妹頻頻點頭…

沃德：「可是，我真的沒有啊…」

這時偉柏和電腦老師說完話後，剛好走到爭論不休的他們身邊，聽完他們的對話，沉思了一會，嚴肅地說道：「原來如此，照這樣看來沃德的電腦應該是中毒了，而且臉書帳號應該是被別人盜用了，所以…」

沃德：「怎…怎麼會這樣…」

（二）問題討論

1. 你覺得駭客為什麼要入侵沃德的帳號？
2. 你知道要怎麼做，才能避免這樣的情形發生？
3. 如果是你遇到這種狀況，你會如何處理？



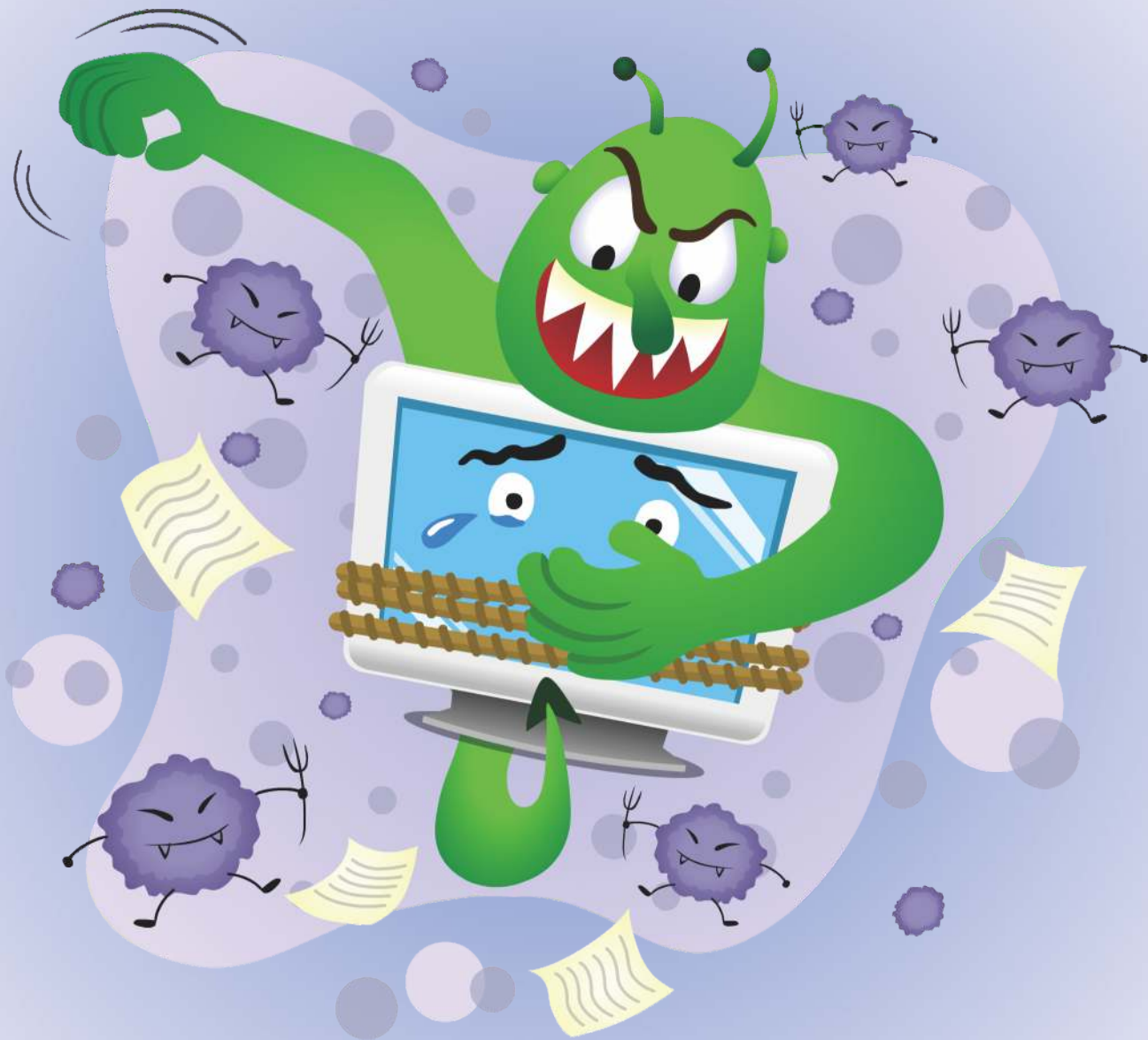


一、認識電腦病毒

維基百科對於電腦病毒的描述如下：電腦病毒（或稱計算機病毒）是一種在人為或非人為的情況下產生的、在用戶不知情或未批准下，能自我複製或執行的電腦程式；電腦病毒往往會影響受感染電腦的正常運作。

教育部的「資安小字典」則指出：電腦病毒會自我複製，並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，但病毒也有可能潛伏而不作任何動作，直到時效到達的那天才進行惡意行為。電腦病毒兩個最重要的行為是「自行複製」與「感染、挾持其它程式」。

簡單的說，電腦病毒其實也是一種應用程式，只是通常它是在您不知情或沒有經過您允許的情況下，進行偽裝（假裝成另一個正常程式）、自我複製、感染甚至刪除其他檔案等傷害電腦系統的事；有些只是惡作劇，有些則會竊取您的個人資料用來從事不法的事情，有些甚至會惡意地造成您的電腦系統損壞或故障！



二、電腦病毒的種類

一般而言我們將電腦病毒分為以下五類：

(一) 木馬/殭屍網路(特洛伊木馬)

特洛伊木馬程式（木馬程式）就像神話中所述的一樣，看起來像是一件禮物，但結果卻是一些突擊特洛伊城的希臘士兵，當使用者被引誘開啟程式時，木馬程式即會散佈開來，攻佔使用者的電腦，進行蒐集情資、等待時機執行破壞任務、當作跳板進行滲透等惡行。

有些也叫作「遠端控制軟體」，如果木馬能連通的話，那麼可以說控制者已經得到了遠端電腦的全部操作控制與許可權，操作遠端電腦與操作自己電腦基本上沒什麼大的區別；因此，使用者的電腦一旦感染了特洛伊木馬，就會成為「殭屍」電腦，成為任駭客擺布的「機器人」。



（二）有害軟體

又稱惡意軟體、惡作劇軟體等。例如：蠕蟲病毒，也是我們最熟知的病毒，通常在全世界範圍內大規模爆發的就是它了，它們會自行複製，利用系統與網路的漏洞，傳播到網路上的任何一臺連接的電腦上，造成網路、系統的癱瘓。

間諜軟體或流氓軟體，係指沒有經過使用者同意的狀態下，自動安裝並無法解除安裝的軟體，且安裝後會惡性破壞其他程式正常運作的軟體。部份不良網路公司出品的一種收集使用者瀏覽網頁習慣而制訂自己廣告投放策略的軟體，可能會綁架使用者的瀏覽器首頁、搜尋列和各種設定，或者是廣告軟體，也可能是有間諜行為，但是都是令使用者困擾的惡意程序。

（三）指令碼病毒（巨集病毒）

巨集病毒的感染對象為Microsoft開發的辦公系列軟體Office，例如：Microsoft Word、Excel 這些辦公軟體本身支援執行可進行某些文件操作的巨集命令，所以也會被隱藏在Office文件中含有惡意的巨集病毒所利用。它們可以跨平臺感染，與一般的執行檔病毒不同。利用Word所提供的巨集功能來感染文件，在網路上已發現不少的文件巨集病毒，流傳速度很快，而且很容易學習，因此以後的發展量將有可能會持續增加。



（四）檔案型病毒

從字義上來看，就是純粹感染檔案的病毒，所感染的檔案類型大部份是可執行檔，如COM、EXE、SYS、BAT、OVL等。當使用者中毒之後，只要再執行其他的程式，病毒就會把自己複製到程式之中，如此不斷的複製與感染，病毒便可以永久生存下去。檔案型的病毒較難加以清除，因為檔案型病毒的感染方式有千百種，而且很可能一次就有好幾百個檔案中毒。

至於近來造成許多使用者的FB、Line等社群帳號被盜、被駭的情形，則是有心人士利用可以安裝外掛（擴充模組）的Firefox、Chrome等瀏覽器，將惡意程式偽裝成正常的外掛應用程式，誘騙使用者授權安裝並藉機取得社群權限，進而盜取使用者個資或以使用者名義進行標記、文章張貼…等未經允許的動作。

（五）進階持續性滲透攻擊(Advanced Persistent Threat, APT)

簡單的說就是針對特定組織所作的複雜且多方位的網路攻擊。攻擊特色有鎖定特定目標、假冒信件、低調且緩慢、客製化惡意元件、安裝遠端控制工具、傳送情資等。APT可能持續幾天、幾週、幾個月，甚至更長的時間。

三、如何防範電腦病毒

- (一) 重要資料一定要備份於不同的儲存媒體
- (二) 安裝防毒軟體並定期更新病毒碼
- (三) 定期做系統及軟體的更新，如Windows Updates
- (四) 只從信任的網站下載檔案
- (五) 不開啟來路不明的郵件、訊息或檔案
- (六) 掃描插入的隨身碟
- (七) 只安裝合法的擴充程式
- (八) 注意社群網站的權限與安全設定



4 四通八達

- 一、透過網路下載檔案時，要注意什麼？
- 二、電腦上的哪些檔案需要備份？如何備份？
- 三、如何處理朋友傳來的訊息或電子郵件的附件？
- 四、電腦中毒後應該如何處理？



5 五彩繽紛

參考資料來源 >>



1. 中文維基百科 <http://zh.wikipedia.org/wiki/電腦病毒>
線上百科全書，資料豐富且即時更新，本篇目包含有電腦病毒的歷史、種類、預防方法等，資料齊全頗富參考性。

2. 吳清基、林宜隆等（2006）。
資訊素養與倫理－國小版。臺北市：臺北市政府教育局。
由臺北市政府教育局出版，內容包括導論、網路禮節、網路識讀、網路詐騙與色情、小小創意家－著作權法、不當資訊、網路交友、網路資料保護、線上遊戲與沉迷、數位達人－網路公民。



3. 吳清山、林宜隆等（2009）。
資訊素養與倫理－國小2版。臺北市：臺北市政府教育局。
<http://ile.tp.edu.tw>
由臺北市政府教育局出版，以培養國小教師及學生資訊倫理、安全與健康的認知與實踐，正確使用資訊網路行為與態度，進而增強預防網路對師生的負面影響。內容包括：資訊停看聽－數位達人、資訊小博士－網路識讀、火星仙子－網路禮節、數碼寶貝－網路詐騙與色情、小小創意家－著作權法、駭客剋星－不當資訊、行遍天下一網路交友、網路不上身－網路資料保護、全民公敵－線上遊戲與沉迷以及數位達人－網路公民等單元。





4. 海芋小站 <http://www.inote.tw/2009/02/blog-post.html>
[閒聊] 常見預防電腦病毒方法！知名的科技部落客網站，經常提供實用軟體教學，介紹有趣網站及資訊，分享程式設計心得，網站資料豐富。



5. 教育部資安小字典 <http://cissnet.edu.tw/Dict>
教育部建置的「校園資訊安全服務網」，提供各級學校有關資安政策、訊息、技術等相關的資料，其中的「資安小字典」係以英文字母排列，簡單扼要的解釋關於資安的一些專有名詞。



6. 學習加油站 <http://content.edu.tw>
此為「教育部數位教學資源入口網」，蒐集了許多關於數位教學的教材與資源。



7. 認識電腦病毒
http://content.edu.tw/junior/computer/tp_ct/content7-b11.htm
介紹電腦病毒的種類與成因，值得參考。



【學習結語】

資訊科技流暢用，未來學習雲端遊；
良好習慣若建立，病毒駭客莫憂愁。

【語詞解釋】

1. 數位原住民與數位移民：

美國的媒體大亨梅鐸在對美國報紙編輯學會的一場演講時，自稱是個數位移民(Digital Immigrant)。他對一出生就活在隨時隨地可以上網的寬頻世界的新生代，則以數位原住民(Digital Natives)稱之。

2. 儲存媒體：

或稱儲存設備、儲存裝置，泛指用來保存電子資料的一切媒體、裝置與設備；目前一般電腦常用的有：硬碟(HDD)、固態硬碟(SSD)、隨身碟(USB flash drive，又稱拇指碟、快閃碟)、隨身硬碟、記憶卡、可寫入DVD光碟、可寫入藍光(BD)光碟、NAS網路附加儲存設備以及網路(雲端)硬碟等。

3. 防毒軟體：

防毒軟體(Antivirus software)是用來偵測、移除電腦病毒、電腦蠕蟲和特洛伊木馬程式的應用軟體。

【MEMO】





網路版



APP版

駭客不上身-病毒防護

【黑長尾雉】簡介：

黑長尾雉為臺灣的特有種鳥類，棲息在具有杜鵑及竹林的茂盛林下層的森林。會吃蕨類嫩芽、嫩葉、野草莓及昆蟲。雄鳥非常獨特，在翼上及尾上覆羽有各種不同的白斑，下背及腰為深黑色，而不是淺藍色。



資料來源：臺北動物園保育網

http://newweb.zoo.gov.tw/Pager/ZooData_Index/ZooData_Index_Show.aspx?Animal_ID=144