

如何避免隨身碟中毒?

預設當電腦偵測到 USB 裝置時，Windows 作業系統會自動尋找並執行 autorun.inf，進而執行其他應用程式。USB 病毒主要利用 autorun.inf 將病毒植入電腦主機，或反向從遭感染的主機把病毒散播到各種 USB 介面的儲存裝置中。以下提供幾個避免隨身碟中毒的方法供使用者適情況使用，以降低中毒機率。

1. 關閉隨身碟自動開啟的功能：在隨身碟插入電腦前，暫時或永久停止電腦的自動播放功能的方法。
2. 新增 autorun.inf 資料夾：事先在隨身碟上設定好，以避免隨身碟遭病毒寫入的方法。
3. 安裝隨身碟防毒軟體：電腦上先安裝好防毒軟體的方法。

關閉隨身碟自動開啟的功能

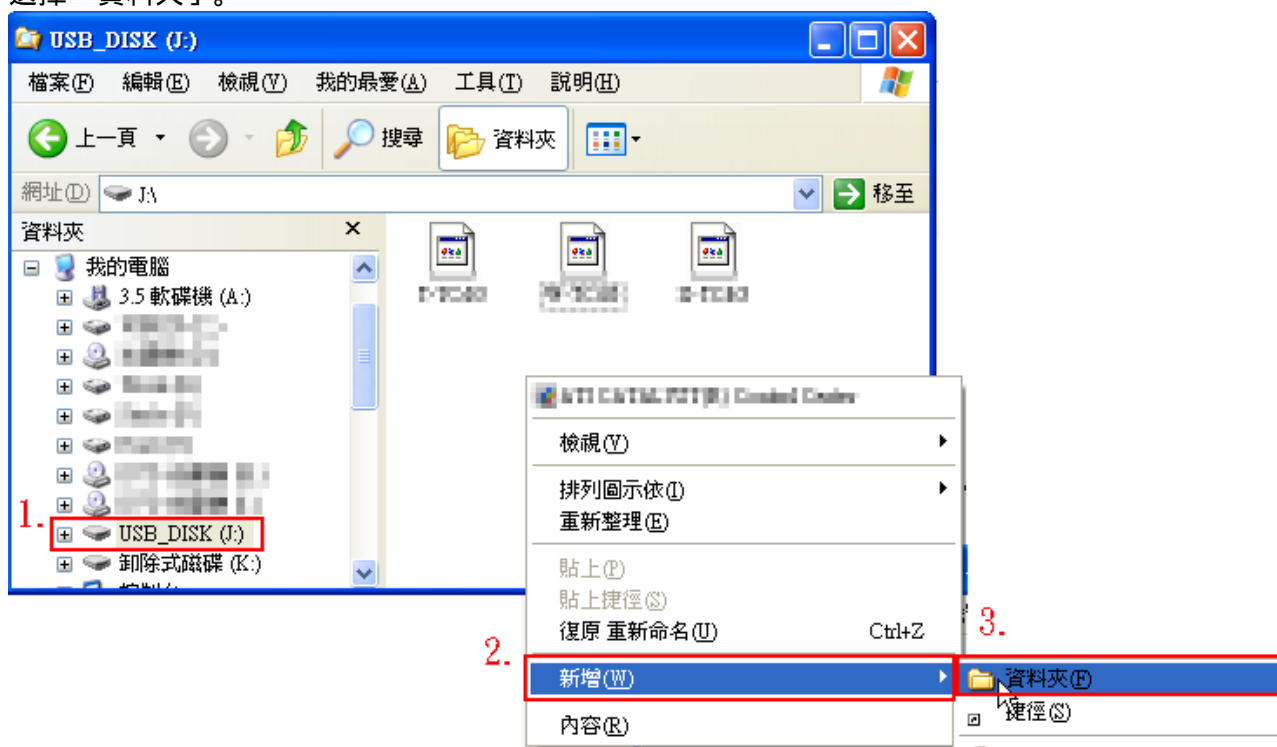
- 詳情請見「[如何關閉自動播放隨身碟或光碟機的功能?](#)」

新增 autorun.inf 資料夾

- 當隨身碟插入已感染 USB 病毒的電腦時，病毒會在隨身碟中製作一個名為 autorun.inf 的檔案，因此利用 Windows 作業系統「在同一個目錄中不能同時存在相同名稱的檔案或資料夾」的特性，預先在隨身碟的根目錄下做好一個名為 autorun.inf 的資料夾，當病毒欲將有害的資料寫入 autorun.inf 的檔案時，因事先已建立好的同名資料夾，就不能順利感染隨身碟了。其製作步驟如下：

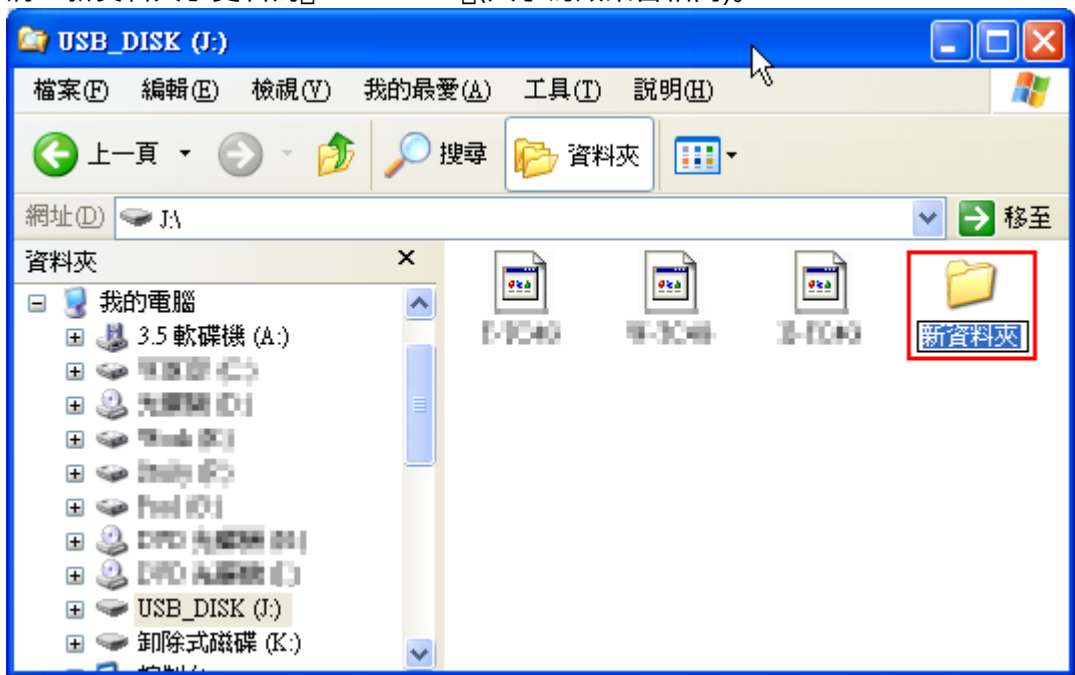
Step 1

1. 選擇要處理的隨身碟，下圖以隨身碟 J: 為例。
2. 在隨身碟的資料夾中的空白處按右鍵，點選新增。
3. 選擇「資料夾」。

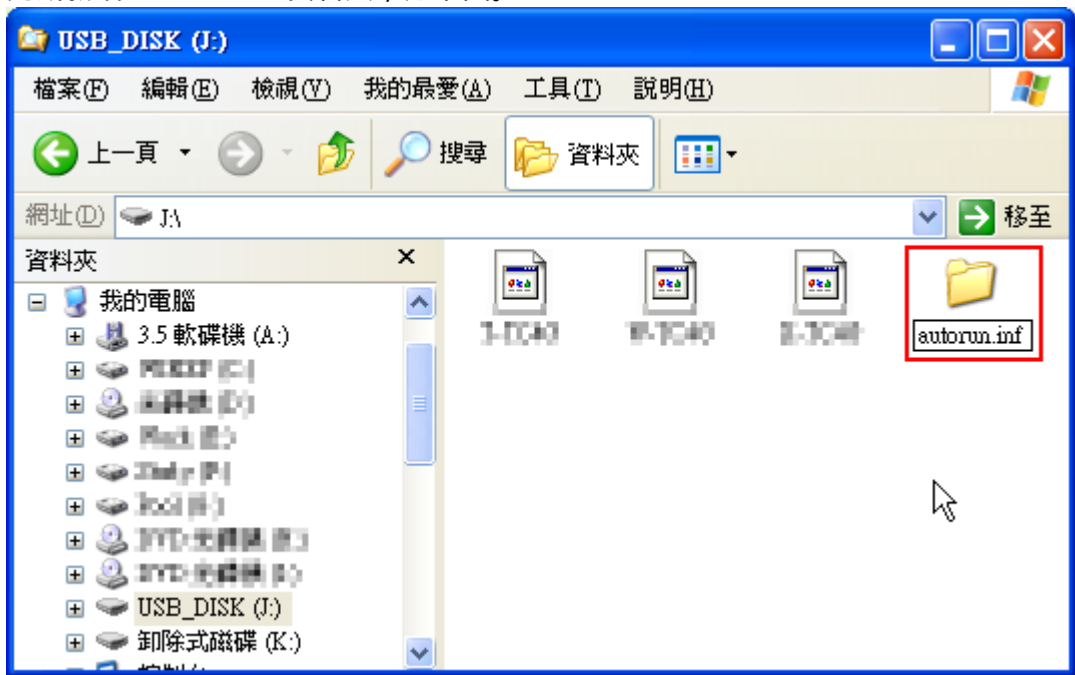


Step 2

1. 將「新資料夾」更名為「autorun.inf」(大小寫效果皆相同)。



2. 完成新增 autorun.inf 資料夾，如下圖。

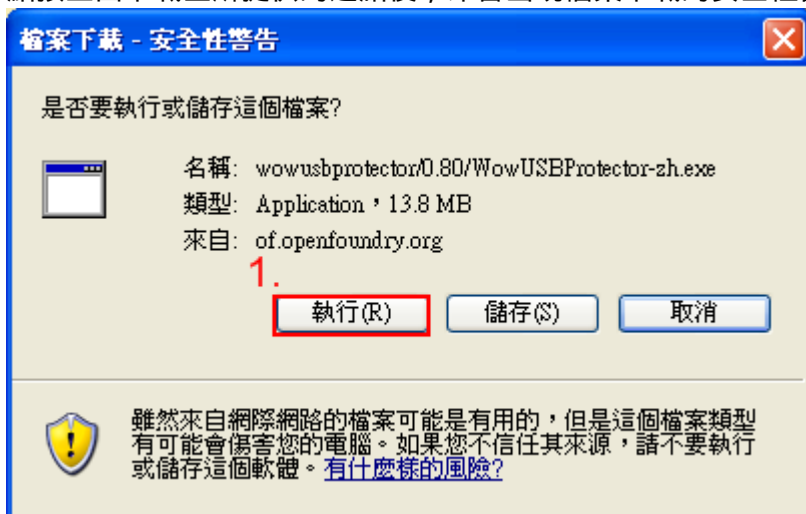


安裝隨身碟防毒軟體

- 此處簡介中研院所研發的可攜式儲存設備防毒偵測之自由軟體其安裝與使用。
 - [Wow! USB Protector 可攜式儲存設備防毒軟體下載區](#)
 - [Wow! USB VirusKiller 可攜式儲存設備防毒軟體下載區](#)

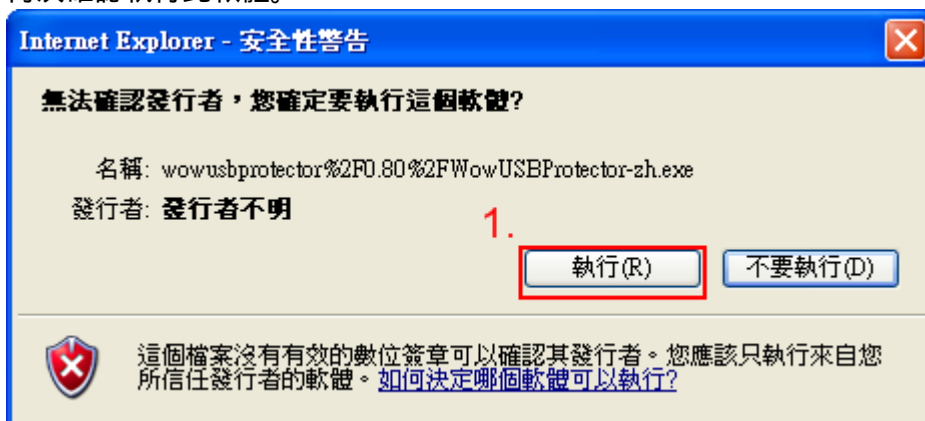
Step 1.

1. 點按上面下載區所提供的連結後，即會出現檔案下載的安全性警告，依下圖選取執行。



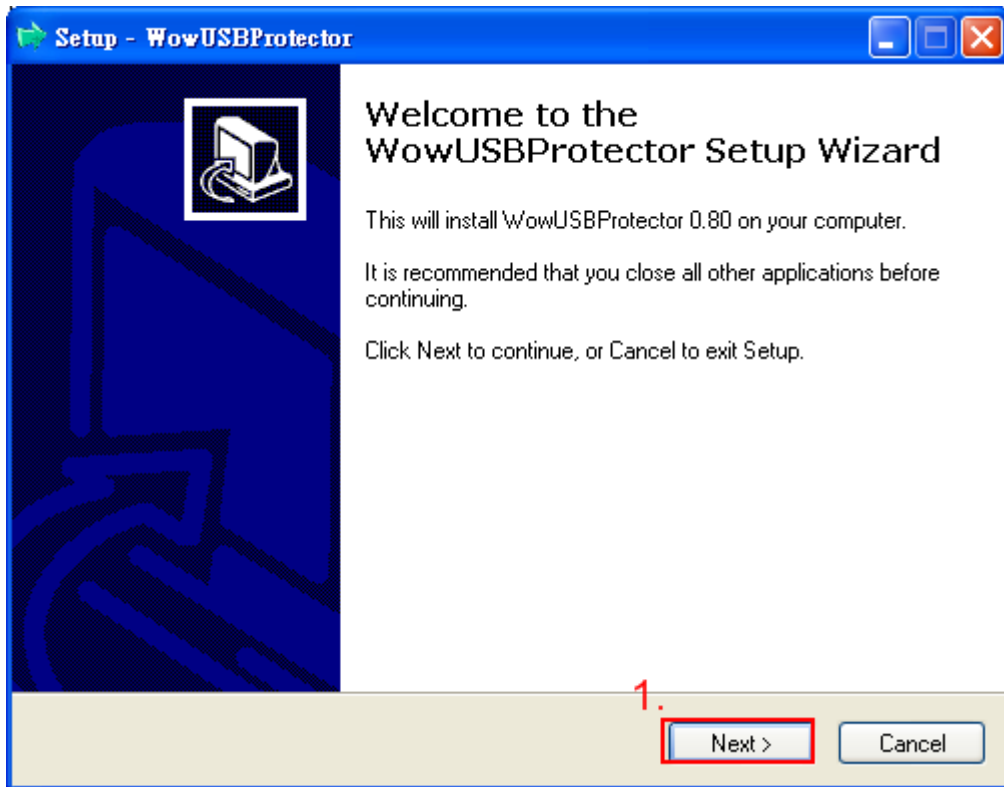
Step 2.

1. 再次確認執行此軟體。



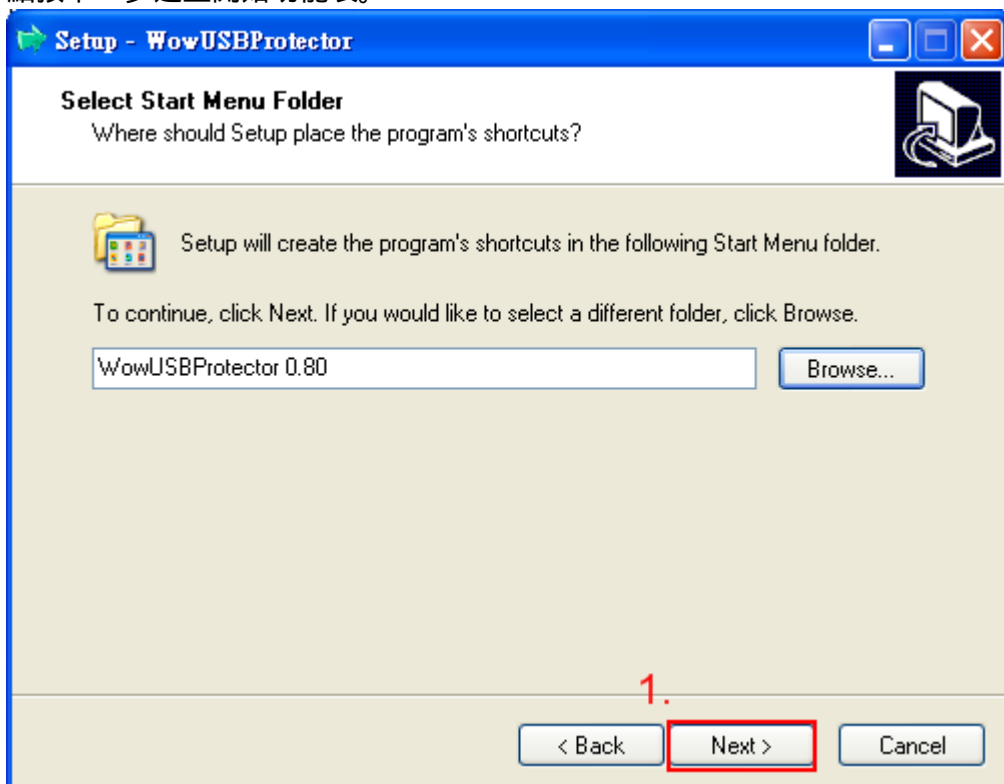
Step 3.

1. 點按下一步安裝開始。



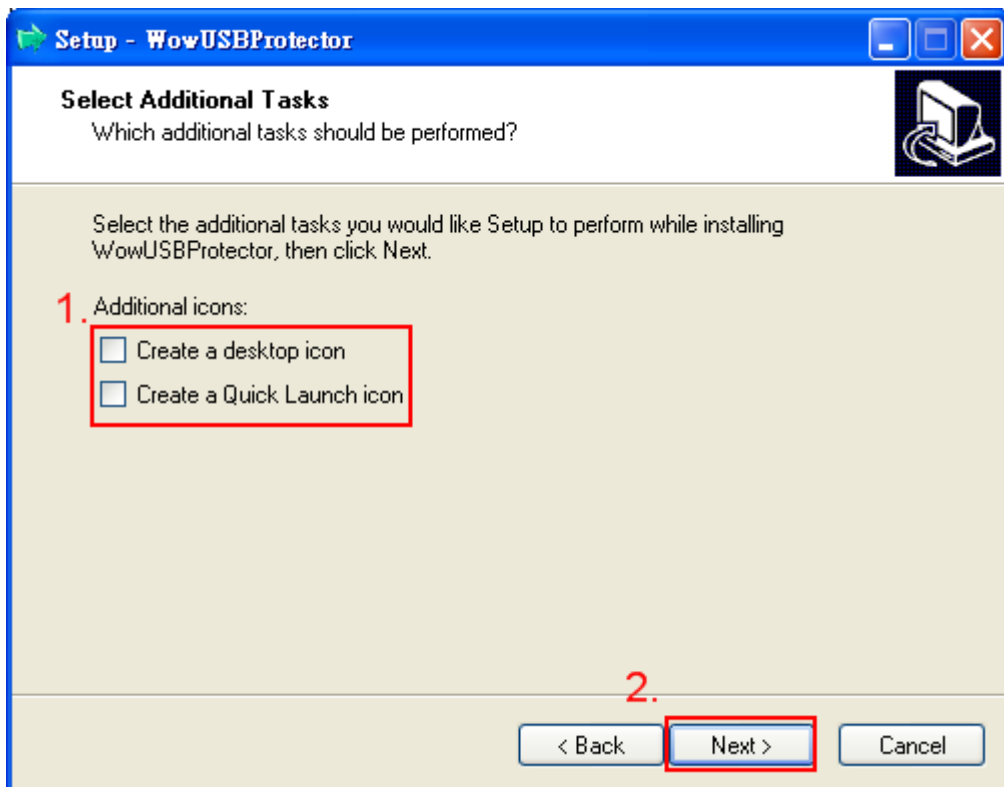
Step 4.

1. 點按下一步建立開始功能表。



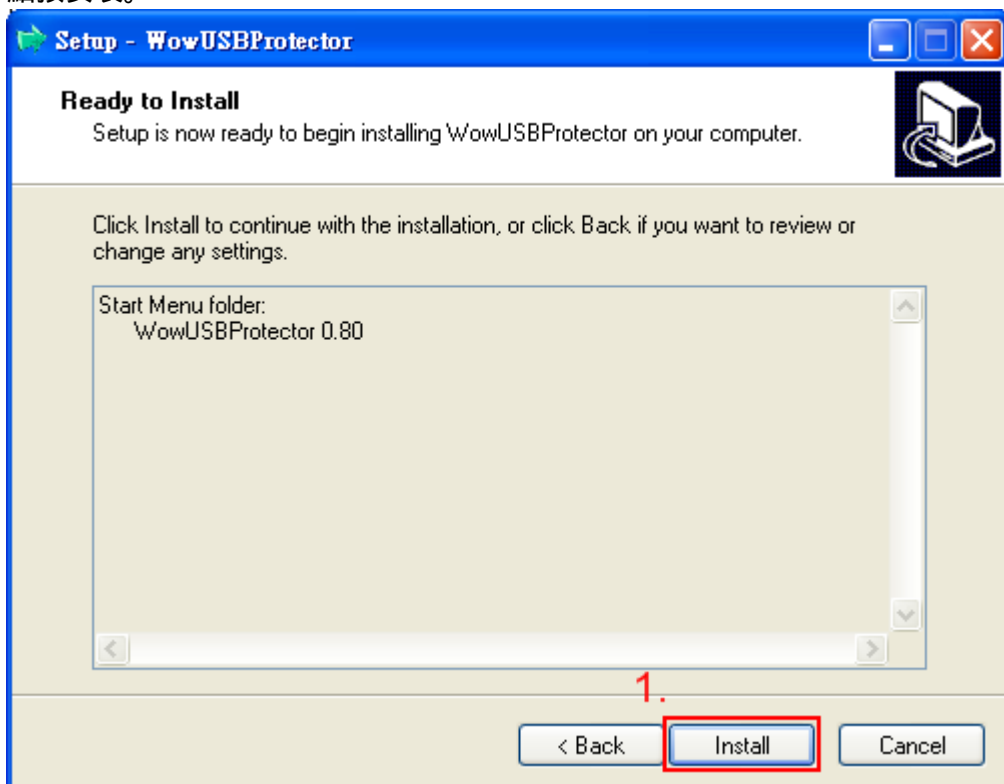
Step 5.

1. 選擇是否要有桌面及快速捷徑。
2. 點按下一步。



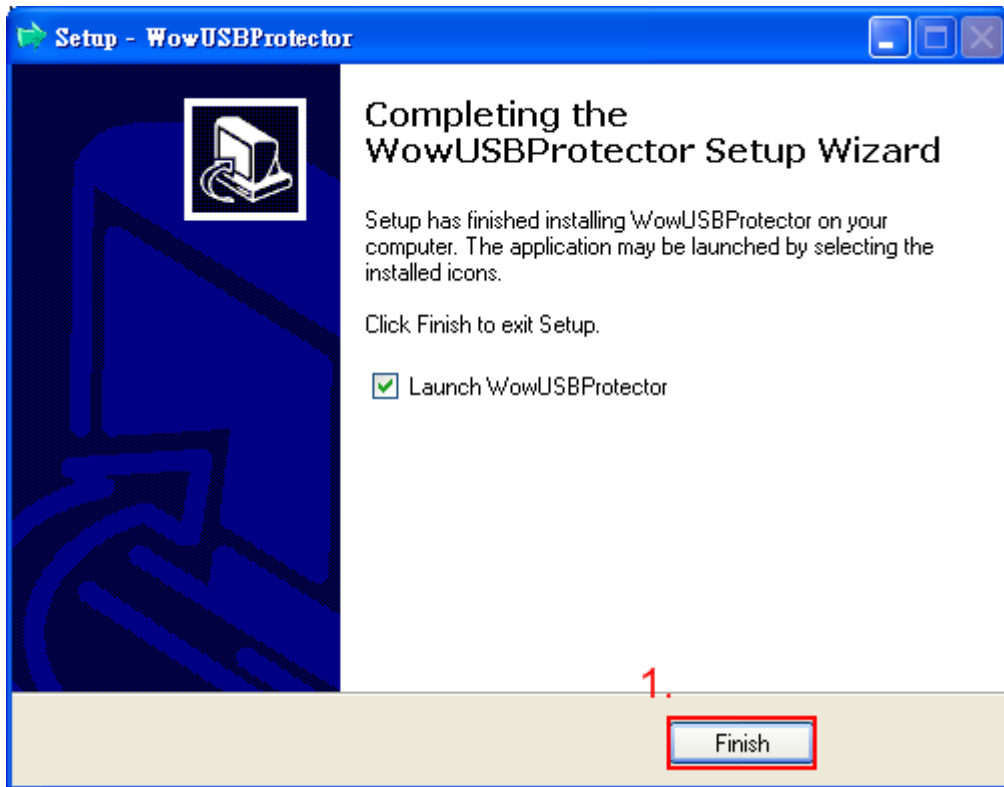
Step 6.

1. 點按安裝。



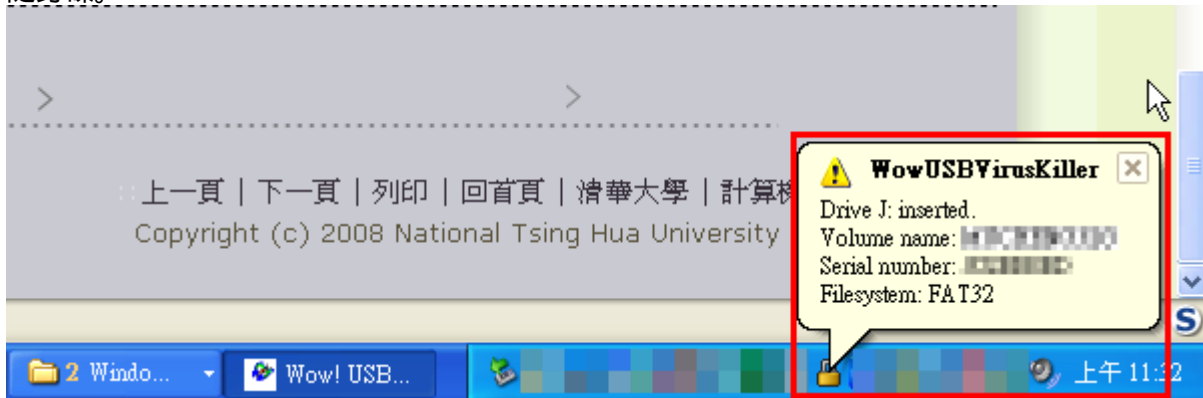
Step 7.

1. 完成安裝。



Step 8.

1. 當隨身碟插入電腦後Wow! USB Virus Killer 偵測到後，電腦右下角顯示如下圖，並開始進行掃描該隨身碟。



2. 若沒有發現病毒，則出現下圖告知使用者。



參考資料

1. [\[\[\[\]\]\]隨身碟病毒防制方法](#) 行政院主計處電子處理資料中心

From:

<http://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:

http://net.nthu.edu.tw/netsys/faq:usb_virus

Last update: **2009/08/10 12:47**

