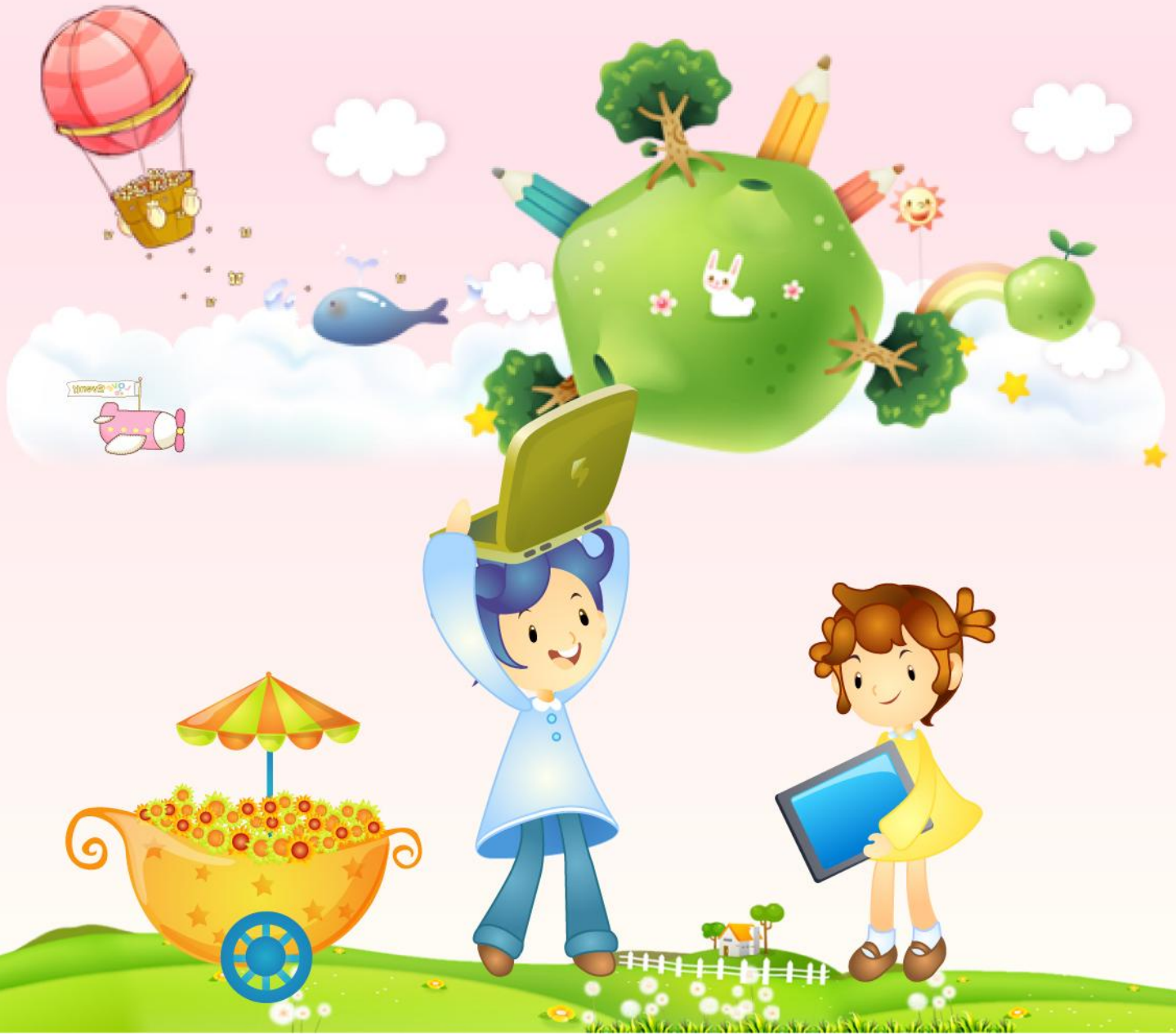
教孩子幫 3C 安檢　爸媽加油讚 (9)

- 概念篇：連網的桌機、手機、平板電腦都有風險
- 影響篇：電腦或手機中毒不只是系統毀損而已
- 注意篇：防毒、密碼與更新為安全防護基本功
- 法寶篇：養成定期備份資料的習慣



概念篇 連網的桌機、手機、平板電腦都有風險

〔疏忽電腦保護可能讓病毒有機可乘〕無論是在家裡、學校、圖書館、網咖或其他任何地方使用電腦，特別是當有連上網際網路時，孩子們都應該有基本的惡意程式防護觀念；因為若是疏忽，電腦很容易遭受如電腦蠕蟲、間諜軟體、病毒、後門程式、木馬程式等惡意程式的侵入。

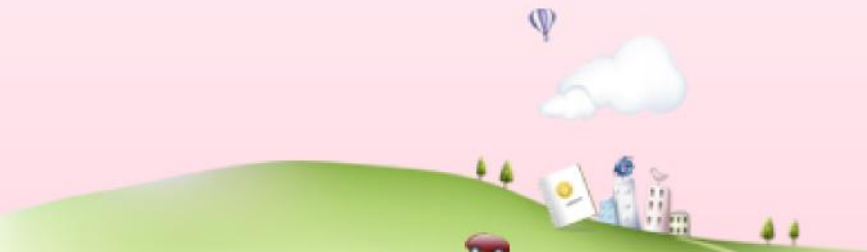
〔惡意程式是未經允許安裝的軟體〕簡單說，惡意程式是一種未經使用者允許就自行安裝到電腦或手機系統內的軟體，可能會攻擊系統、竊取或竄改資料、或透過操作受害者的裝置來從事犯罪行為。惡意程式也可能會自我複製、自我傳播，這也是我們常聽聞，電腦病毒會快速散播與感染的原因。

〔行動裝置和電腦一樣會中毒〕孩子們可以連上網際網路的裝置越來越多樣化，像是平板電腦、智慧型手機等行動裝置，也都和一般桌上型或筆記型電腦一樣，有被植入不同類型惡意程式的安全風險，必須加以注意。尤其是當家中家長和孩子們共用這些 3C 產品時，可能因為孩子不瞭解相關風險與正確的操作方式因而下載了惡意程式，連同家人存放在相同裝置中的重要資訊也可能一併遭殃。

〔社群網路最常用來誘騙下載惡意程式〕大部分的惡意程式會經由用戶點選偽裝過的超連結，下載到用戶端的電腦或手機，這些超連結過去會隱藏在電子郵件中，例如：偽造的領獎通知、有趣影片超連結等。現在則是因為社群網路與 Apps 的流行，有心人士開始大量運用像是假造粉絲團活動、或假借好友名義發布病毒連結等社群網路相關的管道，誘使網友點選這些看似無害卻又包藏禍心的超連結。

臉書流傳「瘋了！我不敢相信，自己看看吧!」為題的影片，點選後即中毒

當點擊以此為標題的超連結(多半會搭配情色圖片吸引點擊)，使用者會被帶往影片播放頁面，並跳出 Flash Player 安裝請求；一旦安裝，該惡意程式會綁架使用者的臉書帳號，並且自動貼上惡意網址擴大影響範圍。 【摘自 T 客邦 2013.3.15】



〔養成定期安全檢查的習慣〕不只是孩子，家中的每一位成員在使用智慧型手機、桌上型或平板電腦等 3C 產品時，都應養成定期幫這些裝置進行安檢的習慣，以避免受到惡意程式的騷擾，像是定期進行病毒掃描、定期更換密碼等。

影響篇 電腦或手機中毒不只是系統毀損而已

〔電腦裡沒有重要資訊不代表中毒沒關係〕許多孩子可能覺得自己不會這麼倒霉，會電腦中毒，或者覺得反正自己的電腦或手機裡沒有重要資訊，中毒也無所謂。其實，這些都是不正確的觀念，特別是智慧型手機，裡頭通常都存放了自己和親友的個人資料，像是通訊錄、簡訊、App 傳訊紀錄(如 LINE 的文字或照片訊息)等屬於隱私資訊，有心人士可能會取得用於不法或詐騙用途。有些惡意程式不只會影響被感染的電腦或手機而已，還會再依被害者的通訊錄，將病毒繼續散播出去，讓親朋好友也因此遭受攻擊。

〔電腦或手機感染病毒的症狀與後果〕下表整理了幾個常見的電腦或手機感染病毒的症狀與可能後果；當發現自己原本正常運作的電腦或手機出現這些常見的異常現象時，可能代表已經被植入惡意程式，這時可能必須求助於提供相關維修服務的專業廠商來協助進行問題的判斷並採取補救措施。

症狀	可能原因	後果
• 上網流量異常增加。	• 可能因為惡意程式正在偷偷蒐集受害者電腦或手機中的有價值資訊，例如：帳號與密碼、銀行或信用卡號碼等，再透過網路將這些資料送到攻擊者手上。	• 攻擊者可利用所偷取到的有價資訊，進行犯罪或詐騙等活動，例如：信用卡盜刷、網路銀行假冒身分登入轉帳等。

症狀	可能原因	後果
• 速度變慢或經常當機。 • 莫名無法開機或無法關機。 • 儲存空間突然不夠。	• 惡意程式隱藏在電腦或手機的記憶體中且不斷自我複製、或大量複製文件，直到系統無法承受； • 惡意程式開啟大量檔案。	• 電腦或手機無法再開機與使用。
• 接到朋友的抱怨，說你的 email 或手機在亂發病毒信或病毒簡訊。 • email 寄件備份中，多出一些不是自己寄的信件。 • 沒有寄出 email 給他人卻收到退信。	• 惡意程式會利用受害者名義發出大量垃圾郵件、散發病毒、或傳送簡訊給通訊錄中的所有人。	• 自己的 email 或手機成為駭客拿來再攻擊他人(傳送病毒) 的跳板。 • 收到大筆金額的手機簡訊帳單。

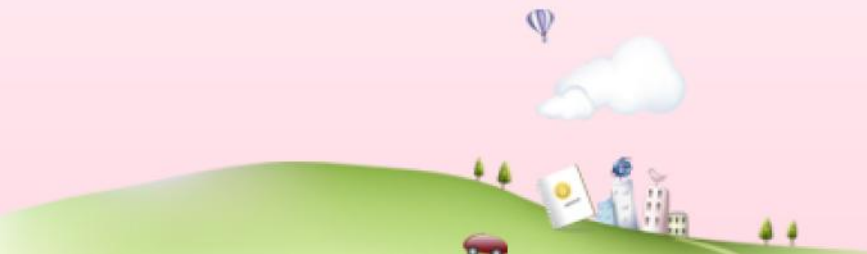
山寨版防毒軟體是惡意程式，暗地啟動 Webcam 拍照再勒索

英國出現會控制使用者電腦的假冒防毒軟體，該惡意程式會控制用戶電腦的網路攝影機拍照，再將照片寄給用戶警告病毒已開始運作，須購買完整版防毒軟體才能解毒。許多受害者一看到自己被偷拍的臉孔出現在電腦螢幕上，便會驚慌地交出自己的信用卡號碼，讓駭客得逞。**【摘自網路資訊雜誌 2013.12.2】**

注意篇 防毒、密碼與更新為安全防護基本功

下列包括螢幕上鎖設定、安裝防毒軟體、以及定期更新電腦軟體等作法，是 3C 安全防護的最基本功夫；建議家長可協助或教導孩子進行相關的設定，以降低遭受到惡意程式威脅的機會。

基本功	操作說明
設定手機與電腦的螢幕上鎖密碼	當不使用手機或電腦時，設定必須輸入密碼才能夠繼續使用的安全上鎖機制，例如：智慧型手機可設定在不使用數分鐘後自動鎖定螢幕，需有正確「數字密碼」或「圖形密碼」後方能開啟。最重要的是，這些密碼必須要不容易被他人猜到，且同時自己又記得住的優質密碼。
為電腦安裝防毒軟體	為家中的電腦安裝防毒軟體，並開啟自動更新病毒碼功能，且定期進行掃描，才能確實阻隔電腦病毒。家長和孩子也都必須了解，防毒軟體並非滴水不漏，有防毒不代表可以肆無忌憚地從網路下載檔案。 縱使手機病毒數量逐年成長，有關智慧型手機是否須安裝防毒軟體，目前還沒有很肯定或一致的建議，可能是因為目前這些手機板的防毒 Apps 尚未有明顯的防範效果。教導孩子不隨便安裝 Apps 或點選超連結，或許是更有效防堵的方式。
絕對不點擊來路不明的超連結	大部分惡意程式能夠入侵成功，是因為使用者開啟了網路上的不明連結、或下載了不明檔案所造成；無論使用電腦或智慧型手機，都應當對來自於陌生人的 email、傳訊、或社群網路的留言所包含的超連結、附夾檔，抱持著警覺，特別是當看到聳動標題時，合理懷疑與小心求證才是上上策。
更新系統與軟體	大多數有規模的軟體公司或手機製造商，都會針對其作業系統(例如：電腦的視窗系統、手機的 Android 或 iOS 作業系統等)、及應用程式(例如：電腦的文書處理軟體、手機的 Apps) 漏洞不定期提供修補程式，並通知用戶下載進行更新，以確保系統與應用程式可因應演化瞬息萬變的惡意程式。 家長可協助孩子定期檢視是否有更新檔(許多軟體會在[說明]選單下，會有[更新軟體]或[查詢更新]的功能)，或設定自動下載更新功能，以確保電腦或手機中的系統與應用程式為最新狀態，降低新安全威脅可能帶來的風險。



1. 沒有百分百惡意程式阻絕的保證

當家裡的大小朋友都已熟悉且能夠實際操作包括前段落所提到的防毒、密碼與更新等安全防護基本功，已可大幅降低電腦與手機遭惡意程式攻擊的機率與風險，但卻無法百分百保證安全無虞。像是防毒軟體無法辨識的全新駭客攻擊手法、孩子不小心點擊了最信任好友傳來的遊戲分享詐騙超連結、從官方 App 市集仍下載到惡意 Apps 等情境，還是有可能會發生。

2. 教導孩子養成備份資料的正確觀念

試著想像電腦或手機中儲存孩子多年的成長照片或影片紀錄、或者孩子苦心用電腦完成的作業，一旦因為中毒而硬碟毀損救不回來時，是多麼令人懊惱的事。針對惡意程式破壞或竊取電腦與手機內儲存的重要資料事件，可於日常就進行資料備份，也應教導孩子瞭解並養成資料備份的觀念，在資料毀損時，方能夠將資料回復原狀，降低衝擊。

3. 備份資料檔案不要存放在同一裝置內

最簡單的備份方式就是把電腦或手機中的檔案複製出來，例如：儲存到隨身碟、光碟片或另外一個硬碟；近期相當流行的雲端硬碟或網路儲存空間，也都是存放備份資料的不錯選擇。無論是選擇何種備份資料儲存媒體，有幾個重要觀念是要注意的：

- ◎ 不要將備份資料存放在同一個硬碟的不同資料夾中，電腦硬碟受損時可能會不分資料夾，全部的資料都毀損；部分智慧型手機可額外裝記憶卡，則可以考慮將資料存在記憶卡中。
- ◎ 妥善地保管備份資料的儲存媒體，例如：不要隨身攜帶以免遺失；若存放私密資料，則可考慮檔案加密，或至少將儲存媒體放置於安全儲存櫃中。
- ◎ 定期進行檔案備份，若家中電腦或手機內的重要檔案每天都會變動或增加，則可以考慮更頻繁的備份頻率，例如：至少每個星期備份一次。家長和孩子們也可以共同訂出一個容易記憶的備份日，例如：每個月的第二個週六下午，使備份成為規律的日常活動之一。

教孩子幫 3C 安檢　爸媽加油讚 (9)

出 版 者　教育部

發 行 者　蔣偉寧　教育部部長

召 集 人　梁理旋　財團法人中華民國國家資訊基本建設產業發展協進會協理

指導委員　楊鎮華　教育部資訊及科技教育司司長

劉文惠　教育部資訊及科技教育司副司長

林燕珍　教育部資訊及科技教育司高級分析師

許雅芬　教育部資訊及科技教育司數位學習科程式設計師

劉玉珍　教育部資訊及科技教育司數位學習科程式設計師

審查委員　林杏子　國立高雄大學資訊管理學系教授

撰稿人員　梁理旋　財團法人中華民國國家資訊基本建設產業發展協進會協理

承辦單位　財團法人中華民國國家資訊基本建設產業發展協進會

出版日期　103 年 3 月

其他類型版本說明　無

※ 此手冊內容係對特定議題所提供之學習教材，僅供各界參考，非本部相關政策。