

## 花蓮縣政府 函

地址：970270 花蓮縣花蓮市府前路17號  
承辦人：陳毓倫  
電話：(03) 8462860#509  
傳真：(03)8577524  
電子郵件：allenc@mail.edu.tw

受文者：花蓮縣秀林鄉三棧國民小學

發文日期：中華民國110年6月28日

發文字號：府教課字第1100126668號

速別：普通件

密等及解密條件或保密期限：

附件：2021030120210623資安封鎖清單、2021020120210623中毒封鎖清單

(376550000A\_1100126668\_ATTACH1.ods、376550000A\_1100126668\_ATTACH2.ods)

主旨：檢送本縣「110年度1月至6月各校電腦資安封鎖清單與中毒封鎖清單」(如附件)，請依說明事項配合辦理，請查照。

說明：

- 一、依據教育部校園網路使用規範及105年09月22日臺教資(四)字第1050103217B號臺灣學術網路管理規範辦理。
- 二、各校資訊組長(資訊教師)檢視(附件清單)後，登入智慧網管系統(<https://snm.hlc.edu.tw/>)協助該台電腦使用者完成解除封鎖，若該台電腦使用者無故拒絕處理請校內依規定流程檢討處理。

### 三、封鎖清單說明：

(一)封鎖清單：泛指教網中心網管或學校資訊老師以「手動封鎖」設備之清單。

(二)如何查詢：登入智慧網管後，點選左方功能列倒數第二「封鎖清單」。

110/06/28



1100002201



(三)封鎖清單：封鎖的要件是已經明確中毒或被植入木馬主動發起電腦攻擊或入侵行為，事態較緊急就會手動封鎖。

#### 四、資安封鎖回報說明：

(一)名詞解釋:C&C(Command & Control Server)伺服器，一

般是指揮控制僵屍網路botnet的主控伺服器，用來和僵屍網路的每個感染了惡意軟體(malware)的宿主機進行通訊並指揮它們的攻擊行為。

(二)資安封鎖：只要電腦有跟C&C清單中的伺服器建立連結，就會封鎖。 說明：學校資訊老師們常會發現，怎麼教職員去了某些站台，就被封鎖，然後可能去比對，這些站台都不在C&C清單上(例如影音網站、購物網站....)。然後可能會想這個清單不準確.....  
但實際

狀況是：那是因為老師們去的這些站台，裡面的「廣告」有夾著"不當"或"別有用心"的程式碼。這些廣告程式碼有跟C&C清單中的伺服器建立連結，所以就會被封鎖。

(三)解決方式：上班期間請維持公務電腦只運於用公務用途，如為教學所需，請下載 adblock 、uBlock Origin之類擋廣告的chrome 擴充功能插件來使用。

(四)如何查詢：登入智慧網管後，點選左方功能列最後一項「報表」-->最後一項「資安封鎖回報」，設定查詢區段。



(五)申請解鎖： 以教育處採購的卡巴斯基防毒軟體掃描  
確

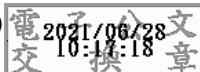
定無病毒(需截圖)及windows更新後，請於智慧網管中  
按下「申請解鎖」填寫回報流程完成後隔天會解鎖。

(六)同一個MAC解鎖後，7天內發生再次對外攻擊事件被封  
鎖： 電腦：需重灌設備、安裝防毒，並於2日後才可申  
請解鎖 其他設備：請通知原廠商處理或拆除，並於2日  
後才可申請解鎖。

(七)同一個MAC 2次解鎖後，14天內再發生對外攻擊事件  
被封鎖：需請資訊廠商使用原版windows光碟重灌完成  
並安裝防毒軟體，再填寫表單回報<https://forms.gle/wM4oVEVkXWhUv9>

五、以上說明請參閱連結網址：<https://reurl.cc/gW4Dp7>

正本：本縣各公立國民中-小學、花蓮縣立體育高級中等學校、國立東華大學附設實驗  
國民小學

副本：本府教育處(教育網路中心)  2021/06/28 10:44:18