防範勒索軟體CryptoLocker之侵害

資料來源：教育局來函　　授課老師：陳啟聰

一、因勒索軟體CryptoLocker開始入侵臺灣，此軟體透過釣魚郵件入侵，將受害者電腦的重要文件和檔案全數加密，導致檔案無法存取，而且駭客採用高超的加密技術(RSA 2048 bit)，讓受害者無法自行復原，並限期內支付贖金，否則將毀損解密金鑰。

二、此軟體一般目前常見感染途徑，大多以下列兩種方式為主：

(一)電子郵件感染。

(二)網站瀏覽感染。

三、駭客往往利用「釣魚郵件」欺騙使用者開啟附件，並夾帶暗藏惡意軟體的壓縮檔附件，附件檔名還偽裝成xxxxxxxx.pdf.exe，因作業系統隱藏附檔名，容易看成PDF文件而誘騙受害者點選而入侵電腦。

四、為避免遭此軟體之侵害，請務必遵守如下條列自保方法及被駭後的緊急應變措施：

(一)自保方法：

1.不要開啟來路不明的郵件。

2.不要開啟可疑郵件的附件檔案。

3.不點選不明的網頁及網站。

4.定時更新防毒軟體。

5.定時備份重要檔案，落實每天備份和掃毒。

6.作業系統的安全更新。

7.Adobe、java漏洞要隨時更新。

(二)被駭後之緊急應變措施：

1.立即切斷受駭PC的網路，避免災情擴大。

2.更新防毒軟體，清查內網其他電腦，並採取自保措施。

3.搶救還沒被加密的檔案。

4.若有備份，開始復原檔案。

5.評估受害災情，決定是否付贖金取得解密金鑰。

6.用新版防毒軟體清除，或乾脆重灌電腦。

臺北市私立延平高級中學「資訊教育融入學習領域」教學活動紀錄表

學年度 與學期	104　學年度　1　學期	領域 科目名稱	藝術媒體科技
教師姓名	陳啟聰	授課班級	國二 4、8、9
資訊教材 單元名稱	防範勒索軟體 CryptoLocker 之侵害	資訊教材 形式	講義
教學活動概況 (請簡述)	(可針對教材設計、教學方式、教學目標、使用教具、教學流程、教學心得、學生反應、省思等方面描述) 教學目標：使學生了解 1.線上網路釣魚(phishing 英文發音如 fishing 一字)是一種誘騙電腦使用者透過電子郵件訊息或網站提供個人或財務資訊的手段。一般線上網路釣魚的誘騙手段都是從電子郵件訊息開始，看起來就像是來自可靠來源的正式通知，如銀行、信用卡公司或聲譽良好的線上商家。在電子郵件訊息中，收件者會被引導至詐騙網站，並在其中被要求提供個人資訊，像是帳號或密碼。然後通常會用此資訊來進行身分盜用。 2.CryptoLocker 此勒索軟體一般目前常見之感染途徑。 3.自保方法及被駭後的緊急應變措施。		

1. 新進教師(含國高中)須連續兩年(4 學期)實施資訊教育融入學習領域之教學。
2. 每學期以教授一個新單元的資訊教材為原則，同一個班級勿上下學期重複教授同一個資訊教材。
3. 資訊教材之授課時間，每學期每班以 5~10 分鐘為原則。
4. 教學活動紀錄表中之授課班級，以實際有教授資訊教材的班級才填寫。請授課老師提醒學藝股長於教學日誌中記載，俾便將來教育局視導時有佐證資料。
5. 資訊教材單元名稱可以自訂，參考名稱如下：資訊素養、資訊倫理、網路資料蒐集與識讀、網路禮節、資訊犯罪與相關法令、網路沉迷與成癮、網路交易、網路交友與戀情、著作權合理使用、個人資料保護法、網路社群使用、網路霸凌、網路拍賣、數位詐騙、網路隱私、中小學網路素養與認知網站介紹、病毒防護、優質通行碼設定與使用原則、或新興資訊教育議題。
6. 資訊教材形式可以為教案、講義、學習單、PPT、Word、影片等多樣性。
7. 為配合教育局每半年追蹤實施成果，每學期請於第 13 週結束前，將本教學活動紀錄表(紙本)及資訊教材(檔案)，一併繳交至教學資源中心彙整。
   資訊教材檔案名稱格式：學年度-學期-教師姓名-資訊教材單元名稱
   (例如：104-1-陳啟聰-網路霸凌介紹)
8. 資訊教材(檔案)彙整後將置於本校網站供下載與推廣，下載連結處：
   本校中文版首頁→網路服務→資訊素養與資訊安全→本校「資訊教育融入學習領域」教材。
9. 「空白教學活動紀錄表」與「資訊教材參考」，下載連結處：
   本校中文版首頁→網路服務→資訊素養與資訊安全。