防範勒索軟體CryptoLocker之侵害

資料來源：教育局來函

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。