檔　　號：
保存年限：

臺北市政府教育局　函

地址：11008臺北市市府路1號9樓西北區
承辦人：許世杰
電話：(02) 27331838轉13
傳真：(02) 27328484
電子信箱：jbrother@mail.taipei.gov.tw

受文者：臺北市大同區大橋國民小學

發文日期：中華民國104年10月30日
發文字號：北市教資字第10441384000號
速別：普通件
密等及解密條件或保密期限：
附件：

主旨：為宣導防範「勒索軟體CryptoLocker」之侵害一案，請查照。

說明：

一、依據臺北市政府資訊局104年10月27日資安宣導之電子郵件辦理。

二、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。

三、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。

四、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。

五、為避免各校遭此軟體之侵害，請各校加強宣導如下條列自保方法及被駭後的緊急應變措施，請務必遵守：

(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)嫻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。

正本：臺北市立大學、臺北市政府教育局所屬公私立各級學校、臺北市各市立幼兒園
副本：電子公文交換章 2015-10-30 11:25:44