

圖書館公告

依據臺教資(四)字第 1050175317 號辦理，近因部分單位重要系統發生勒索病毒資安事件，致重要資料毀損影響公務正常進行，請勿下載不明來歷軟體。

「臺北市政府各機關勒索病毒防範方法」摘要說明

一、本防範方法對勒索病毒的防護方案分為適用「用戶端」或「伺服器端」，說明如下：

- (一) 適用用戶端及伺服器端：開啟事件檢視器並收集各紀錄檔，以便於感染勒索病毒後，追查感染狀況。
- (二) 適用用戶端：除部分公務系統必須使用 Internet Explorer (簡稱 IE) 瀏覽器外，建議盡量使用 Chrome 瀏覽器，並使用 Adblock Plus 或 Adblock 等擴充工具，以阻擋網頁之內嵌廣告。
- (三) 適用用戶端：使用 Windows Defender 間諜程式掃描工具，並定期更新病毒碼。

二、本防範方法之勒索病毒緊急處理分為一般使用者及資訊人員，說明如下：

(一) 一般使用者：

1. 斷網：斷開網路連線。
2. 斷電：馬上關機，避免加密程序繼續擴大受害範圍 (5 分鐘內或許可救回部分資料，但針對部分勒索病毒無效)。
3. 現場保留電腦並通知機關內資訊人員。
4. 切勿付錢。

(二) 資訊人員：

1. 關閉帳號，暫時停止該帳號的網路存取登入權限。
2. 檢查該帳號權限可以寫入的公用資料夾是否感染。
3. 將硬碟取出，透過另一台電腦備份尚未被加密的檔案。
4. 回收事件檢視器內紀錄。
5. 收集勒索訊息及勒索畫面 (可加快判定病毒類型)。
6. 找出勒索病毒入侵管道。

