

防範勒索病毒5叮嚀

勒索病毒如何勒索？

勒索病毒是一種惡意程式，其散播途徑與一般惡意程式或電腦病毒一樣，一旦感染，它會鎖住受害者的電腦，或者將受害者電腦的硬碟資料加密，進一步要求受害者繳交贖金後，才能夠取回對電腦的控制權或者將硬碟加密解開。以 wannacry 勒索病毒為例，駭客要求的贖金為價值約 300 美元的比特幣。某些勒索軟體會依受害者支付贖金的時間增減贖金，通常越晚支付則贖金的金額會越高；也有些狀況是，即便受害者支付了贖金，電腦也沒有因此被解鎖。

要如何避免資料被綁架？

防範勒索軟體的方式與防範任何惡意程式的方式一樣，平常使用電腦網路的時候應謹慎，以下 5 項提醒事項，可以讓你降低遭受到勒索病毒侵害的機會：

- 1** 不輕易點選email內的超連結，如果真的有必要，建議直接在瀏覽器中輸入你所要去的網站網址。
- 2** 不任意開啟email的附件，除非你知道寄件者並且確定附件內容為何。
- 3** 不要瀏覽名聲不佳的網站，特別是情色影片網站或是盜版電影網站，因為很可能只要瀏覽這些網站就會受到電腦病毒感染。
- 4** 不任意下載任何軟體。
- 5** 定期備份你的檔案或資料在另外一個獨立裝置（如行動硬碟），或者使用雲端硬碟來備份，萬一出事，還可以找回重要資料。