「勒索軟體」之預防

資訊網路使用普及之現代社會，政府機關、企業及個人用戶都須保有正確資訊安全觀念，避免落入惡意軟體多種攻擊陷阱，以維資料及機密之安全。
電腦使用者搭乘網路安全公車（BUS）必經三大站以通往資訊安全的目的地：

定期備份

為了避免重要資料被駭而無法回復的情形，電腦使用者應隨時將重要資料備份至異地，免於遭受勒索軟體威脅。

系統軟體定期更新

電腦使用者須定期更新作業軟體及防毒軟體，以修補系統漏洞，降低遭到勒 索軟體攻擊機率。若防毒軟體偵測出系統已感染，在顯示出勒索訊息前，先切斷主機網路連結，以避免完成加密程序，並重新安裝系統軟體，確保系統及資料安全。

不隨意開啟不明郵件及注意瀏覽網頁安全

不管是公務機關、公司團體或個人使用者，除了倚靠資訊單位防禦管理外， 都必須養成良好的網路使用習慣。不隨意開啟來源不明的電子郵件、附件及自非信任來源下載安裝程式，另瀏覽網頁時，不要開啟網頁上嵌入的廣告連結，避免落入勒索病毒的陷阱，造成個資外洩或更大損害。

面對惡意攻擊不斷演進的網路環境，電腦使用者必須隨時保持警戒，養成良 好的網路安全習慣，避免因為疏忽而造成個人資料被駭及其他相關損害，在浩瀚未知的網路世界，唯有搭乘網路安全公車（BUS）方能通往資訊安全的境界。