小心!假防毒軟體詐騙你的信用卡資料

最早的假防毒軟體係利用恐嚇手法，讓使用者信以爲真的感染警告。不過這個手法的威脅情勢已轉化爲營利爲主，促使網路犯罪份子運用更多的迂迴狡詐的技術，目前最常用的是模仿即時掃毒畫面，並測知目標電腦上執行的作業系統版本，然後跟著調整相對應的詐騙介面，讓使用者誤以爲中毒無法使用，接著出現付費購買防毒軟體方能解毒繼續使用，騙取使用者刷卡付費，既取得信用卡資料又詐騙金錢，提醒民眾注意。

家住新北市的王同學今年 7 月在家使用電腦，因誤觸釣魚網站，導致電腦中毒，隨後頁面出現若要解除，需購買防毒軟體，王同學不疑有他，線上刷卡付費後，還是無法解除中毒，方覺遭到詐騙。由於電腦中毒後先顯示掃毒畫面，之後出現微軟公司的安全性警告以及網路無法執行，再來顯示假的掃毒結果及病毒來源等資料，即便使用者重新開機，電腦畫面顯示的是無法使用的藍底白字的說明畫面，或是假的微軟開機畫面，告知使用者須購買防毒軟體。歹徒以假冒微軟公司的圖像，加上使用者受騙付款後會收到假的解毒軟體及金鑰，更讓民眾無法分辨是否遭到詐騙。

警方呼籲民眾不要隨易點擊來路不明的電郵附件和網路連結，並熟悉自己電腦裡所使用的防毒軟體，包括廠牌名稱、病毒警示視窗，以及更新程式與病毒碼的方法，以及定期更新。如果跳出的警示視窗的廠牌標示，與所使用的防毒軟體不同，那就很有可能是假防毒軟體。此外，沒有一款防毒軟體會採用付費掃瞄及清理電腦的方式，請民眾勿輕易上當，有任何與詐騙相關疑問，歡迎撥打 165 反詐騙諮詢專線查證。