《資安漫畫》預防勒索軟體綁架－

三不三要

資料來源：中央研究院資訊服務處
趨勢科技全球技術支援與研發中心

一封冒稱健保局的「二代健保補充保險費扣繳辦法說明」，導致萬筆中小企業個資遭竊，登上媒體版面；報導指出史上最大美政府 400 萬筆個資遭竊；可能導因於駭客將病毒電郵偽裝成同事間電郵，誘使收件人開啟；無獨有偶 員工誤開有毒郵件，日本國民年金機構外洩 125 萬筆個資！日本國民年金機構對外證實，由於職員使用電腦時開啟含病毒的電子郵件，導致機關內保存的國民年金相關個資外洩，目前已確定有 125 萬筆國民個資外洩。最近大舉入侵台灣的勒索軟體 Ransomware 也經常使用類似的社交工程（social engineering）信件的手法，達到綁架電腦的目的。比如趨勢科技部落格報導過的這篇勒索軟體假冒 Chrome、Facebook 和 PayPal 發網路釣魚電子郵件，或是以下資安漫畫所提供的"假鎖定帳號，真勒索"的真實案例。

預防勒索軟體綁架電腦三不三要		
不上鉤	不打開	不點擊
標題特別吸引人的郵件務必停看聽	不要隨便打開 email 附件檔	不要隨意點擊 email 夾帶的網址
要備份	要確認	要更新
重要資料要備份	開啟電子郵件前要確認寄件者身分	病毒碼一定要隨時更新

如何避免自己成為勒索程式的受害者？

儘管 勒索軟體 Ransomware 相當危險，但只要提高警覺，隨時留意 勒索軟體 Ransomware 的最新動態，對於保護資料和電腦就有很大幫助。以下是一些防範這類潛在攻擊的實用秘訣：

開啟電子郵件之前請先仔細看清楚

小心不明來源的電子郵件，您可直接向寄件人求證他們是否寄了這樣一封訊息給您。

避免點選不明來源電子郵件內的連結

這類社交工程（social engineering）信件技巧經常會導致使用者下載到勒索程式。此外，還要小心那些要求您輸入圖片中文字的網站，因為它們可能暗藏 勒索軟體 Ransomware 攻擊。

備份您的重要檔案

雖然預防重於治療，但若您的重要檔案都已備份，您至少可以將 勒索軟體 Ransomware 的傷害降至最低。雖然系統被鎖住還是一件不幸的事，但至少不會是一場災難，因為您還可以復原重要的檔案。請遵守 3-2-1 **備份原則**：*3* 份備份、*2* 種不同儲存媒體、*1* 個不同的存放地點。