當心！別讓自己成為電腦勒索的受害者

您為電腦做好防護準備了嗎

鼎基提醒您

注意電腦使用安全及勿點勿上不明連結及網站

一台工作站受害，將危及全公司的電腦及主機安全

史上最狠的勒索軟體已在全球各地肆虐，臺灣企業也成了攻擊標的，陸續傳出受災消息。

近期接獲客戶受害案例，**受害人員開啟不明連結網站，或未安裝防護設備、掃毒系統未定期更新..等**，以致遭受感染，使用者若不願支付贖金時，資料將全部鎖死，最後只能將受害電腦全部重新安裝，但資料將無法恢復及使用。

攻擊途徑

- 假冒重要文件，使用偽裝連結，開啟惡意網站
- 透過附件檔案，誘使受害者開啟惡意程式
- 在被挾持的傀儡電腦安裝惡意程式
- 以等級加密技術將受害電腦的檔案加密鎖死
- 勒索受害者支付，以贖回解密的密碼
- 限時付款，否則銷毀解密私鑰，檔案將無法救回
- 透過Bitcoin(比特幣)虛擬貨幣匿名交易機制付款

自保方法

- 不要開啟來路不明的郵件與附件檔
- 不要瀏覽不安全的網站
- 執行防毒軟體掃描、更新防毒軟體、常用作業系統、瀏覽器和常用軟體
- 限縮檔案分享權限、只開放必要文件或目錄可讀寫，其餘檔案均唯讀
- 落實資料備份，並確保備份檔與電腦隔離（或將備份檔改成唯讀狀態）

IT1 企業電子化技術服務技術
ERP企業資源規劃

AU1 自動化產品設計技術
電腦輔助製程規劃

AU4 自動化產品設計技術
MIS規劃及設計

鼎基資訊電腦
DinGey Information Computer Co., Ltd.
台北:(02)2226-6446 傳真:(02)2226-6505
台中:(04)2261-4775 傳真:(04)2263-9375
高雄:(07)350-3299 傳真:(07)350-3630
http://www.dingey.com.tw

經濟部工業局技術服務能量顧問團隊為您電腦化健診

續背面

內部資安管理

資料安全、通訊安全及記錄、郵件安全、權限控管、防COPY、防大量儲存及列印、病毒防範、系統備份/還原重建回復等備份及救援回復…。

網路架構建置

防火牆、網路架設、網管交換器、內部的各項網路設定、MAIL郵件管理、二岸三地資料管理、遠端連線及資料傳輸、主機資料庫、AD授權使用、WiFi及無線網路管理…等網路安全建置服務。

外部入侵偵測

預防外部侵入取得資訊，判斷為入侵者或是誤用系統資源之使用者，並針對異常的網路活動及特徵，擴充系統的檢測範圍，讓安全架構提供有效安全防護。

資訊安全管理解決方案實務案例：

[駭客入侵]電腦存取變慢，經網管人員測試發現，外部網路駭客不斷測試公司資料庫帳號密碼，導致網路變慢，影響效能也產生資料安全問題。

[解決方案]**防火牆**可防止未允許的連線，建立安全的網路邊界並分隔網路區段，為遠端用戶存取內部資源，建立安全性通道。

[中毒木馬]電腦中毒，被植入木馬竊取資料，並在使用者不知情下操縱電腦，發佈大量垃圾郵件及進行網路詐騙。

[解決方案]**防毒軟體**使用於偵測、移除電腦病毒、電腦蠕蟲和特洛伊木馬。含有即時程式監控識別、惡意程式掃描和清除和自動更新病毒資料庫等功能。

歡迎來電，將由專業資安顧問提供諮詢服務!!