公務機密 資訊安全維護

網路無國界，個資須警戒。

一.不輕信誇大廣告並填寫個資

二.慎選賣家和購物網站 不隨意匯款

三、收到可疑電話 先詢問165詐騙專線

以上三步驟
順利去網GO

資安時事案例

電郵詐騙／駭客新招數 癱瘓機台系統

像蘋果的充電線 一插駭客就能偷你資料

個人資料保護法

個資法規範的行為與對象

輕鬆學資安

Digital Signature 數位簽章

數位學習 105年資安動畫金像獎

資安購GO
https://www.youtube.com/watch?v=b7frOSJJULM

電郵詐騙／駭客新招數 癱瘓機台系統

聯合新聞網　記者何佩儒／專題報導 108.10.11

「Bob，拜託幫我們看一下，我們的機台被癱瘓，已經一再的還原、備份再啟動，但機台還是無法順利運轉，要怎麼辦？」趨勢科技台灣區及香港區總理理洪偉淦近兩年常接到這樣的電話，立刻出發到客戶廠區「救火」。

台積電去年因機台作業系統的漏洞未修補，遭到「想哭」病毒入侵，機台癱瘓損失數十億元。洪偉淦表示，過去駭客攻擊大多是辦公室內的資訊系統（IT），但想哭病毒具有自我傳播能力，會流竄到專用型電腦，也就是運轉系統（OT），包括廠區的機台、排程的主機，甚至自動提款機等，透過加密OT藉此要求企業付款，成為駭客新的獲利模式。

攻擊OT比IT更容易的原因是，很多工廠機台是運轉多年的機器，系統不僅久未更新，事實上也無法更新，因為一更新與新系統可能有相容問題，因此相當脆弱。一旦被攻陷，駭客如入無人之境。

洪偉淦指出，除自動化的機台可能被駭，有些傳統產業的生產線會有電腦控制流程與訂單系統，駭客只要加密這些主機，企業即無法進行排程，就算還原、備份，還是可能反覆被攻擊。甚至機台上有些記錄生產資訊，如料號、數量的記錄器，會將資訊傳回主機，讓企業及買主掌握即時的生產資訊，有時記錄器及主機也會被攻陷，生產線雖然持續運作，但跟「眼睛瞎了」沒兩樣。企業主及買主發現生產資訊大半天不更新，就會很緊張找資訊人員解決。

洪偉淦表示，針對OT的攻擊，當然有方法阻絕，但終究要回到管理問題，老闆要在生產效率及資安間取得平衡。過去對工廠來說，提高生產力是最高準則，現在面對駭客威脅，可能要增加管控流程，犧牲一點生產效率。尤其現在許多企業主都有資安意識，但仍低估資安威脅所帶來的損失。

另外，物聯網（IOT）時代來臨，各種連網的裝置都可能成為駭客工具。三年前美國東岸即因駭客控制大量的網路監視器（IP Cam），發動大規模攻擊，導致包括Spotify、Netflix等服務都受到波及。另外，區塊鏈技術帶動加密貨幣的流通，也有駭客入侵個人電腦，藉此進行挖礦，既耗用使用者的電力，也搶走電腦的運算效能。

▼USB隨身碟不要亂插，免得被駭客盜取資料。（圖／東森新聞）

像蘋果的充電線 一插駭客就能偷你資料

東森新聞

USB隨身碟不要亂插，免得被駭客盜取資料，但現在入侵手法已經演進到充電線，有駭客成功研發出，外觀跟蘋果原廠一模一樣的充電線，但內含惡意晶片與軟體具攻擊能力，只要把這條線插進你的手機或電腦，就能趁機竊取資料。

市面上原廠、副廠的充電線百百種，充電傳輸沒問題，卻有可能會竊取資料嗎？

民眾：「我是覺得不太可能啦，你線只是拿來傳輸充電而已，不可能會有這種動作。」

民眾大呼不可能，但最近在世界駭客大賽上，有一位資安研究員就向聽眾介紹一款自製充電線，外表就跟蘋果原廠充電線一模一樣，讓人無法分辨，線一插上去裏頭內建WIFI晶片就會啟動，讓你的裝置成為WIFI熱點，連線距離最遠可以達到三百英呎，駭客就能趁機動手腳執行指令。

3C專家 Tim：「電腦有可能被他鎖定住，甚至有點像勒索軟體一樣，你要付費才可以解鎖，第二個是你個人電腦所有個資都有可能被他竊取，所以其實是滿嚴重的。」

這種線在市場上，已經出現很長一段時間，其他USB線，也有可能會被利用，據資安人員的了解，甚至可能連美國國家安全局，都有出過自己的版本，因此專家，也提出防範的方式。

3C專家 Tim：「記得還是看包裝上有MFI的蘋果認證，還有比較信賴的品牌，第四個就是如果那個陌生人是你不熟悉的，我建議就不要使用，因為你根本不知道那條線是否晶片已經被竄改。」

如果還是很害怕，那就盡量使用原廠線，避免瀏覽或下載不知名app，自然降低被駭客入侵的機會。

圖解個資法

個資法規範的行為與對象

▶個資法規範的行為

蒐集	以任何方式取得個人資料
處理	為建立或利用個人資料檔案所為資料的記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送
利用	將蒐集的個人資料為處理以外的利用

▶個資法規範的對象

公務機關　非公務機關（包含個人）

公務機關：指依法行使公權力的中央或地方機關或行政法人。

非公務機關：指公務機關以外的自然人、法人或其他團體。

iThome

文 /吳其勳

Digital Signature 數位簽章

參考資料：i-Security

以數位的方式在文件上做「簽名」的動作。利用的原理是訊息最初都會先經過資料結構中的雜湊演算法進行摘要處理後再以個人私鑰（Private Key）加密，最後再由一組公鑰（Public Key）對訊息做第二次加密的動作，特點在於可使文件收取者確認該訊息內容是否有經過未授權的竄改。