優士國際聯合顧問有限公司

資安及個資保護通識教育訓練

于燿彰 博士

2023/07/13

講師簡介

- 學歷:
  1. 國立成功大學 工程科學所 博士
  2. 密蘇里大學堪薩斯城校區 資訊工程所 碩士
- 經歷：
  1. 財團法人電信技術中心 資通安全組 副組長
  2. Hermes-Infortech Inc. 資深資安顧問/講師
  3. 鼎智國際技術服務有限公司 技術長/資深資安顧問
  4. USIS INC. 創辦人/技術長/資深資安顧問 （現任）
  5. 鑑智實相科技股份有限公司 協同創辦人/執行長（現任）
  6. 鑑智實相科技股份有限公司（馬來西亞分公司）協同創辦人/技術長（現任）
  7. 國立成功大學工程科學所 兼任助理教授 （現任）
- 專長:
  1. 網路通訊協定安全
  2. 資訊安全
  3. 管理系統(資訊安全、IT服務、營運持續)
  4. 資安產品測試 (ISO/IEC 15408)
  5. 密碼模組測試(FIPS 140-2)
  6. 實體環境安全
  7. 密碼學
- 稽核員資格：
  1. ISO/IEC 27001稽核員
  2. ISO/IEC 17025稽核員
  3. BS10012稽核員
- 聯絡資訊:
  Email: avis.y@ustar-is.com

大綱

- 資安及個資管理政策宣導
- 社交工程防護宣導
- 資訊安全案例
- 資安法簡介
- 個資洩漏案例
- 個資法簡介

資安及個資管理政策宣導

資通安全政策 (1/2)

●資通安全管理原則

1. 重要之資訊資產應定期清查、分類分級與進行風險評鑑，並實施適當的防護措施。
2. 重要資訊資產存取權限應予以區分，考量人員職務授予相關權限，必要時得採行加解密（例rar）及身分鑑別機制，以加強資訊資產安全。
3. 對於資通安全事件須有完整的通報及應變措施，以確保資訊系統、業務的持續運作。
4. 應訂定營運持續計畫並定期演練，以確保重要系統、業務於資安事故發生時能於預定時間內恢復作業。

資通安全政策 (2/2)

- 資通安全管理原則

5. 相關人員應依規定接受資安教育訓練與宣導，以加強資通安全認知。
6. 定期執行資安稽核作業，檢視存取權限及資通安全管理制度之落實。
7. 違反本政策與資通安全相關規範者，依相關法規辦理。
8. 本政策每年至少評估一次，依業務變動、技術發展及風險評鑑的結果修訂。

資通安全政策-目標

●資通安全目標

1. 確保本校核心資通系統網路機房維運服務達全年上班時間96%以上之可用性。
2. 因資通安全事件、異常事件、其他安全事故造成系統、主機異常而中斷營運服務之情事，每次最長不得超過系統所訂之復原時間目標（recovery time objective, RTO）。
3. 本校核心資通系統服務達全年上班時間98%以上之可用性，本校核心資通系統因資通安全事件、異常事件、其他安全事故造成系統、主機異常而中斷營運服務之情事，每次最長不得超過系統所訂之復原時間目標（recovery time objective, RTO）。

個人資料保護管理政策 (1/3)

●個人資料之保護

1. 本校已成立個人資料保護組織，明確定義相關人員之責任與義務。
2. 本校已建立與實施個人資料管理制度（以下簡稱PIMS），以確認本政策之實行；全體員工及委外廠商應遵循PIMS之規範與要求，並定期審查PIMS之運作。
3. 為防止個人資料被竊取、竄改、毀損、滅失或洩漏，本校資通安全暨個人資料保護推動委員會下設資通安全暨個人資料保護推動小組，規劃、執行各項個人資料保護作業，由本校各單位二級主管及行政人員組成，資通安全暨個人資料保護推動委員會執行秘書兼任組長，並依相關法令規定辦理個人資料檔案及個人資料清冊安全維護及更新。

個人資料保護管理政策 (2/3)

- 個人資料之保護

4. 個人資料檔案應建立管理制度，分級分類管理，並針對接觸人員建立安全管理規範。
5. 為確保所有個人資料安全，應強化個人資料檔案資訊系統存取安全，防止非法授權存取，維護個人資料之隱私性，應建立安全保護機制，並定期查核。
6. 個人資料檔案儲存於個人電腦者，應於該電腦設置可辨識身分之登入通行碼，並視業務及重要性，考量其他輔助安全措施。
7. 個人資料輸入、輸出、存取、更新、銷毀或分享等處理行為，應釐定使用範圍及調閱或存取權限。

個人資料保護管理政策 (3/3)

- 個人資料之保護

8. 本校各單位如遇有個人資料檔案發生遭人惡意破壞、毀損或作業不慎等安全事件，應進行緊急因應措施，並依本校「個人資料保護緊急應變處理作業說明書」通報程序辦理。
9. 本校係以嚴密之措施、政策保護當事人之個人資料，包括本校之所有教職員工生，均受有完整之個資法及隱私權保護之教育訓練。倘有洩露個資之情事者，將依法追究其民事、刑事及行政責任。
10. 本校之委外廠商或合作廠商與本校業務合作時，均應簽訂保密契約，使其充分瞭解個人資料保護之重要性及洩露個資之法律責任。倘有違反保密義務之情事者，將依法追究其民事及刑事責任。

個人資料保護管理政策-目標

●個人資料保護管理目標

1. 依據「個人資料保護法」、「個人資料保護法施行細則」與相關標準/規範要求，保護個人資料蒐集、處理、利用、儲存、傳輸、銷毀之過程。
2. 為保護本校業務相關個人資料之安全，免於外在威脅，或內部人員不當之管理與使用，致遭受竊取、竄改、毀損、滅失、或洩漏等風險。
3. 提升對個人資料之保護與管理能力，降低營運風險，並創造可信賴之個人資料保護及隱私環境。
4. 為提升同仁個人資料保護安全意識，每年定期辦理個人資料保護宣導教育訓練。
5. 定期針對個人資料流程進行風險評鑑，鑑別可承受風險等級。

社交工程防護宣導

為何需要社交工程演練

1. 測試同仁面對社交工程攻擊是否具備有判斷的能力。
2. 提升同仁資安意識使之能有足夠的警覺性培養出更多思考與檢查的習慣。

何謂社交工程

利用人性弱點,
應用簡單的溝通
和欺騙技倆。

獲取帳號、
密碼、
身分證號碼或
其他機敏資料。

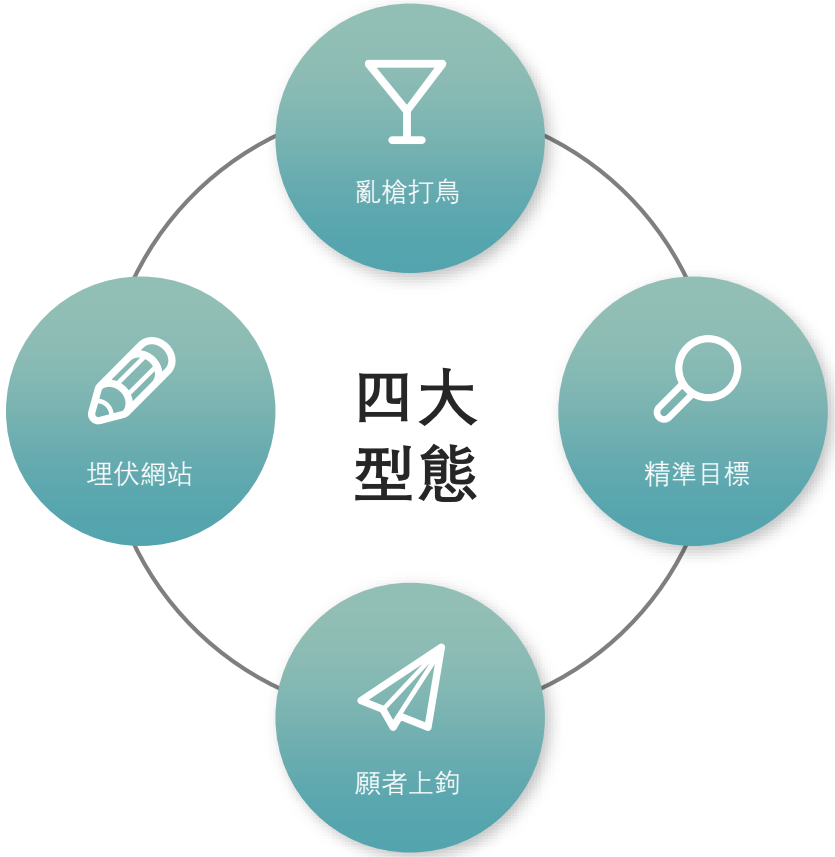
突破企業的
資通安全防護

行非法的存取、
破壞行為

攻擊目的


竊取
機密檔案
及文件
蒐集
針對性
資料
蒐集
使用者
個人資料
竊取
部落格或
社群網站之
帳號密碼
目的
竊取
商業機密
資料
監控
使用者行為
竊取
網路服務之
有價財產
成為跳板、
殭屍電腦

常見的社交工程攻擊型態



亂槍打鳥--垃圾誘餌攻擊

根據社會時事，攻擊者寄送惡意程式郵件或訊息。這些資料訊息的標題通常包含「吸引人」的社會事件。

埋伏網站--水坑式攻擊

先觀察目標習慣瀏覽哪一些網站？接著去入侵網站並植入惡意程式，等待目標對象、造訪網站，再趁機感染惡意程式竊取資料。

精準目標--魚叉式攻擊

針對特定目標或特定機構的員工，觀察其社群媒體帳號，精心製作出很有說服力的手機訊息或電子郵件內容，並且挾帶可造成感染的附件檔或URL連結。

願者上鉤--釣魚式攻擊

先製作假網站，攻擊者寄送電子郵件，誘騙受害者到這些假網站。這些假網站通常偽裝成「金融」或是「信箱」的異常通知。

各種社交工程攻擊手法

偽裝維護人員、
上級單位人員，
騙取帳號及密碼。

利用工具軟體、
檔案、圖片誘騙
下載，乘機
植入惡意程式，
暗中收集
機敏性資料。

利用電話
佯裝資訊人員，
騙取帳號及
密碼。

利用電子郵件
誘騙開啟檔案、圖片，以植入惡意程式、暗中收集機敏性資料。

利用電子郵件
誘騙使用者
登入偽裝網站，
騙取帳號及
密碼。

利用通訊軟體，偽裝親友來訊，誘騙點選連結後，植入惡意程式。

社交工程五大攻擊指標

資料來源：https://www.openfind.com.tw/taiwan/socialengineering/

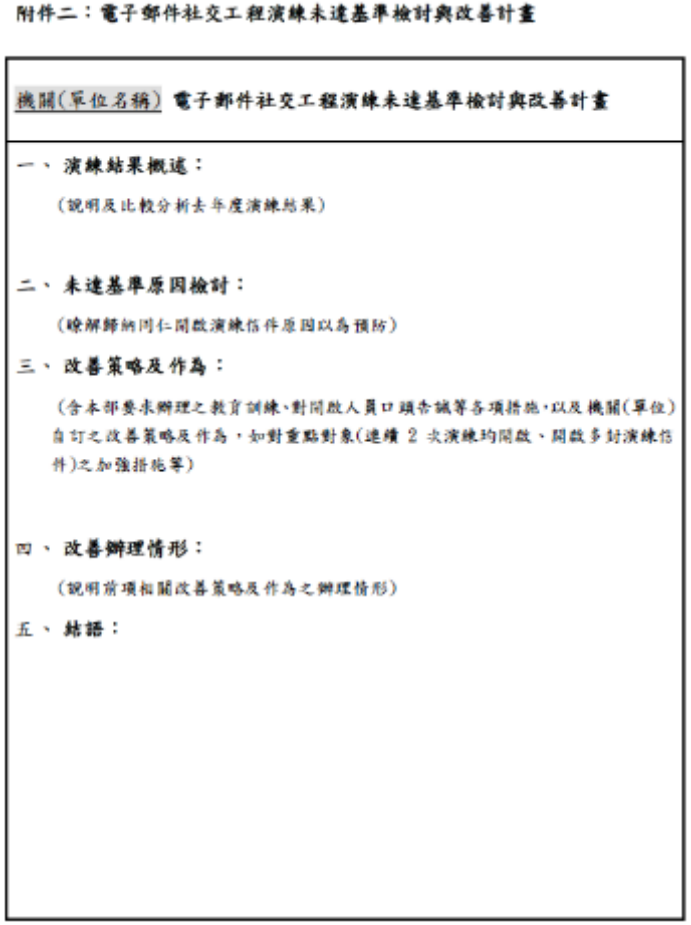
社交工程的共同點

資料來源：趨勢科技

法務部防範電子郵件社交工程施行計畫

法規名稱：	法務部防範電子郵件社交工程施行計畫
公發布日：	民國 97 年 03 月 20 日
修正日期：	民國 108 年 04 月 03 日
法規體系：	法務部部內各單位 > 資訊處
圖表附件：	附圖一：法務部資通安全處理小組組織架構圖（電子郵件社交工程演練作業）.PDF 附件一：演練郵件範本.PDF 附件二：電子郵件社交工程演練未達基準檢討與改善計畫.PDF 附圖二：待改善機關評選流程.PDF 附表：待改善機關評選標準及項目表.PDF
立法理由：	立法總說明 條文對照表.ODT

- 同仁如當年度2次演練均開啟點閱演練郵件，且合計達了封
- (含)以上未改善者，得移送考績會議處。另演練成績未達基準之機關（單位），首長（單位主管）需併同參加至少1小時之補強教育訓



附件二：電子郵件社交工程演練未達基準檢討與改善計畫

機關(單位名稱) 電子郵件社交工程演練未達基準檢討與改善計畫

一、 演練結果概述：

（說明及比較分析去年度演練結果）

二、 未達基準原因檢討：

（瞭解歸納同仁開啟演練信件原因以為預防）

三、 改善策略及作為：

（含本部要求辦理之教育訓練、對開啟人員口頭告誡等各項措施，以及機關(單位)自訂之改善策略及作為，如對重點對象(連續 2 次演練均開啟、開啟多封演練信件)之加強措施等）

四、 改善辦理情形：

（說明前項相關改善策略及作為之辦理情形）

五、 結語：

Facebook當紅　駭客發動釣魚攻擊

網域多為.im/.at或.be　儘快更新系統修補

記者 張中昌 報導 2009-06-16

看準社交網站的高人氣，近來有越來越多駭客，對此發動網路釣魚攻擊！根據賽門鐵克觀察表示，日前再度偵測到新一波網路釣魚攻擊，同樣主要還是針對Facebook使用者，利用受到入侵帳號，寄送含有惡意連結的電子郵件到他人收件匣，藉此誤導登入Facebook的假冒網頁。

▲駭客針對社交網站，進行網路釣魚攻擊(圖/卡優新聞網)

資料來源：網路新聞

近期出現大量針對性網路釣魚攻擊，包括通過Google文檔分享進行攻擊

5月25日消息，推特用戶tayvano_ 發推表示，最近看到有大量十分具有針對性的網路釣魚攻擊，其中最致命的一種是通過 Google 文檔分享來進行攻擊，而且這個分享看起來像是你認識的某個人關於你感興趣的某件事情所發出來的，它不會被標記為垃圾郵件，並且看起來非常真實，注意不要點擊。 慢霧創始人餘弦轉發提醒稱，小心你的電腦被朝鮮駭客等組織投毒，尤其警惕下那些文檔，不管是 Windows 還是 Mac 還是 Linux，也不管你安裝了什麼殺毒軟體。一旦控制了你的電腦，駭客有無數手法盜走你的加密貨幣。

真正的Web3世代？OpenSea研究爆：95% NFT釣魚攻擊由「未成年駭客」發起

by James — 2023-06-20 in 法規, 犯罪 AA

圖源：Boardroom

近年來 NFT 及加密貨幣釣魚攻擊事件頻傳，在過去 9 個月中，至少有 3.2 萬個錢包受害，價值 7300 萬美元的 NFT 和加密貨幣遭竊。OpenSea 信任與安全團隊研究員 Plum 透露，在這些釣魚攻擊中，有高達 95% 是 18 歲以下的青少年，他們還會拿贓款去賭博。

（前情提要：別被騙！OpenAI技術長推特被盜，12.6萬追蹤者見「釣魚連結」騙發幣）

（背景補充：Google搜尋釣魚攻擊暴增！「3千人上鉤」逾400萬鎂加密資產被盜）

資料來源：網路新聞

北韓仿冒南韓入口網站NAVER 發動釣魚攻擊竊個資

法新社 中文新聞
2023年6月14日

（法新社首爾14日電） 南韓國家情報院（國情院）今天表示，北韓模仿南韓最大入口網站NAVER，製作了一個釣魚網站來竊取個資。

北韓製作的釣魚網站網址為www.naverportal.com，網站首頁的即時新聞等版面設計跟真實網站雷同，目的是竊取南韓NAVER用戶的帳號密碼，讓平壤當局獲得珍貴的個人資料。

國情院在聲明中說：「北韓駭客對我國人民的攻擊手法愈來愈精細，我們籲請民眾提高警覺。」聲明並稱當局已對南韓用戶封鎖該釣魚網站。

聲明提醒：「若您看到非NAVER標準網域的網頁，請立即停止連線。」

NAVER是南韓最大科技公司之一，提供類似於Google（谷歌）地圖、Apple Pay的服務，以及人氣部落格與聊天論壇等多種功能，許多南韓人每天都會使用NAVER。

南韓外交部今天也宣布，為強化因應北韓網路活動，外交部決定與美國網路安全公司麥迪安（Mandiant）加強合作。麥迪安是Google的子公司。

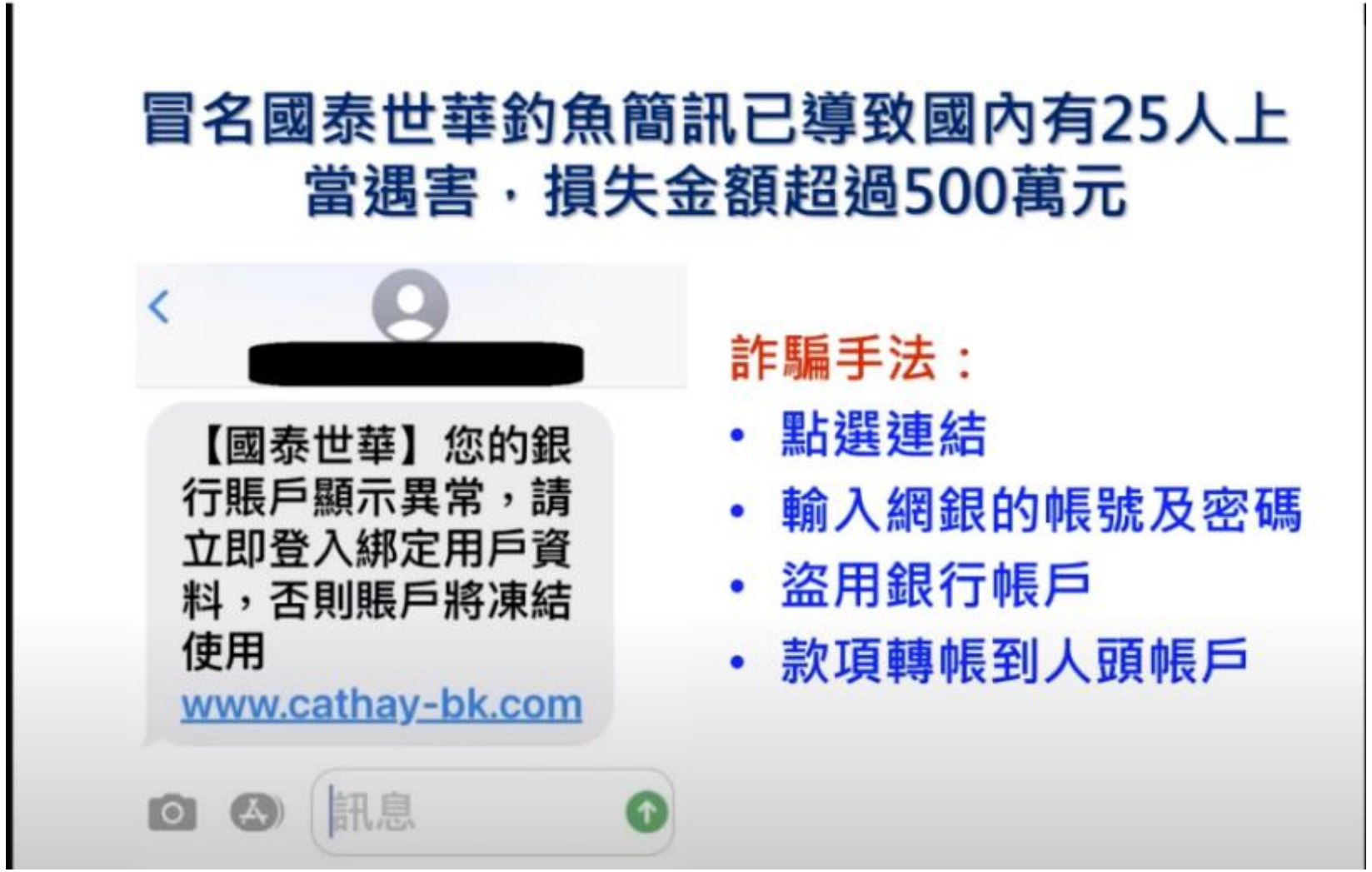
【網絡釣魚】Walmart最受攻擊者歡迎高佔16%　物流、科技及金融成三大目標

商業 17:47 2023/04/27 讚好 2

網絡安全廠商Check Point發表《2023年首季品牌網路釣魚報告》，報告顯示物流、科技及金融品牌位列全球網絡釣魚攻擊三大目標行業，零售巨頭Walmart更於本年首季位居榜首，佔所有網路釣魚攻擊16%，排名自去年第四季的第13位大幅上升。

按照網路釣魚攻擊中的總出現率排序，最常被冒充的品牌是Walmart (16%)，其後則是DHL (13%)、Microsoft (12%)、LinkedIn (6%)、FedEx (4.9%)及Google (4.8%)。

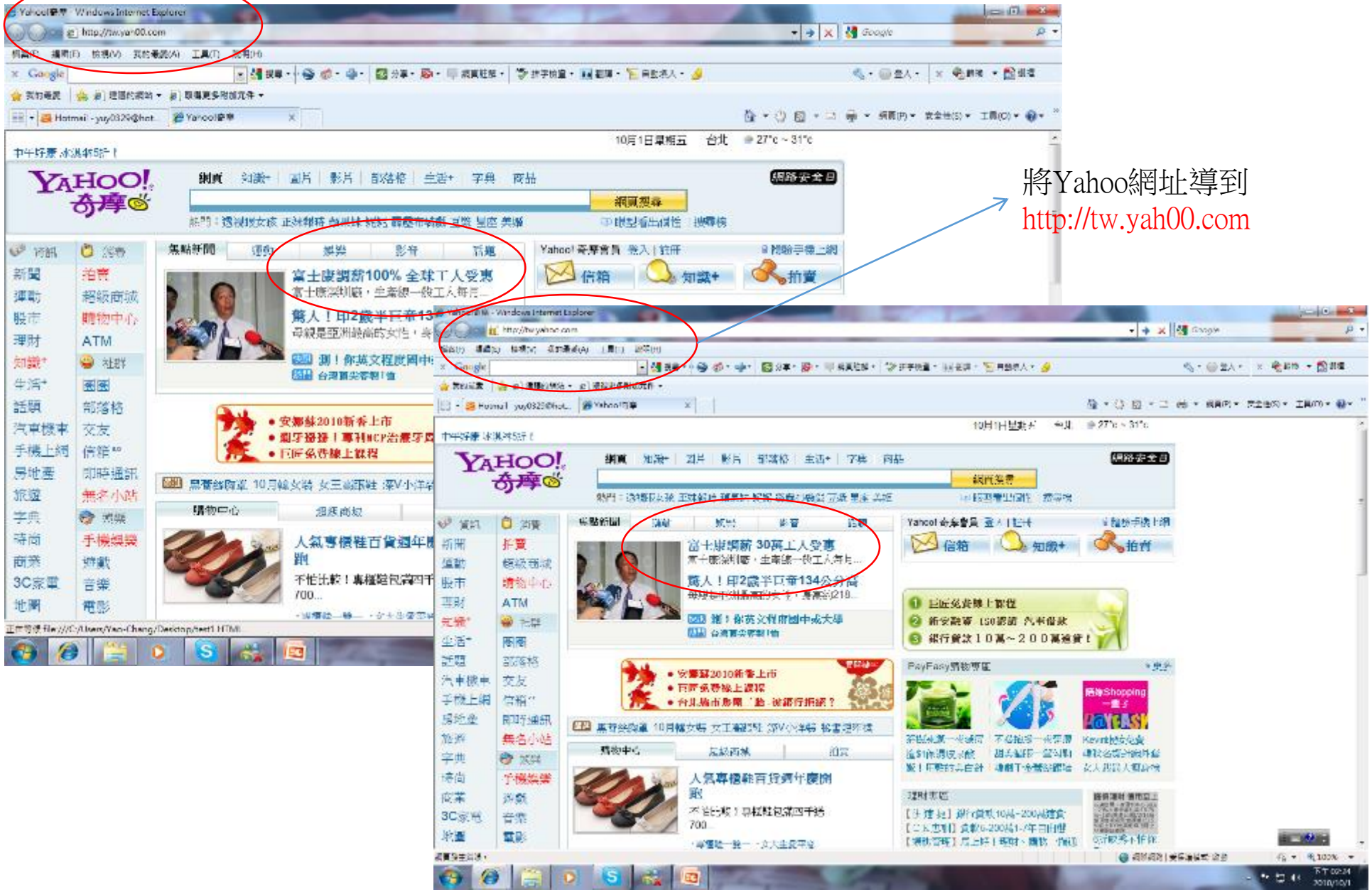
資料來源：網路新聞

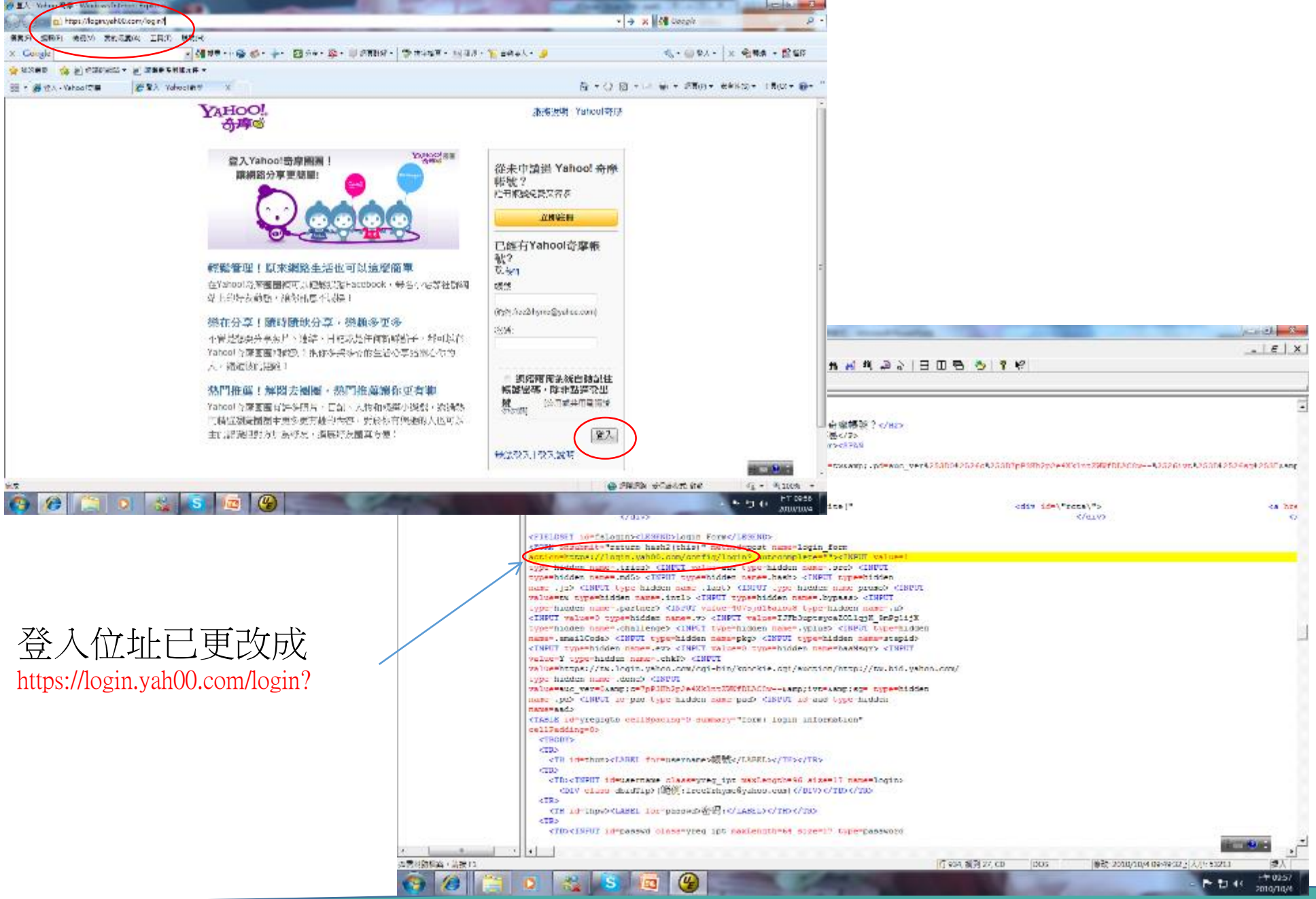

冒名國泰世華釣魚簡訊已導致國內有25人上當遇害，損失金額超過500萬元
【國泰世華】您的銀行賬戶顯示異常，請立即登入綁定用戶資料，否則賬戶將凍結使用
www.cathay-bk.com
訊息
詐騙手法：
點選連結
輸入網銀的帳號及密碼
盜用銀行帳戶
款項轉帳到人頭帳戶

資料來源：網路新聞

詐騙-網路釣魚


http://yahoocom.w52.10te.net/yahoo.com.tw/tw/action/c434256867/
YAHOO! 奇摩
Yahoo!奇摩 - 服務說明
歡迎使用Yahoo奇摩
快樂購物盡在 Yahoo!奇摩購物中心
使用免費的電子信箱及即時通訊。
使用反間諜軟體及網頁跳窗阻擋，保護您的電腦安全。
了解您所在地區的天氣及目前溫度。
隨時更新！最新的音樂、娛樂、體育消息。
Yahoo!奇摩將為會員不斷推出新服務
加入Yahoo!奇摩會員，馬上就可以享有電子信箱、即時通訊、拍賣、購物通、交友、家族等服務 — 完全免費！
登入Yahoo!奇摩
如何保護帳號？
立刻開啟安全圖章 (說明)
帳號:
(範例:free2rhyme@yahoo.com)
密碼:
記住我的帳號密碼(說明)
登入
無法登入 | 登入說明
還沒有Yahoo!奇摩帳號?
註冊帳號免費又容易
立即註冊


將Yahoo網址導到
http://tw.yah00.com



登入位址已更改成
https://login.yah00.com/login?

惡意電子郵件常見攻擊手法

假冒寄件者

利用與業務、聳動的時事電子郵件主旨

含惡意程式的附件

利用應用程式之弱點，包括零時差攻擊

電子郵件停看聽-收信

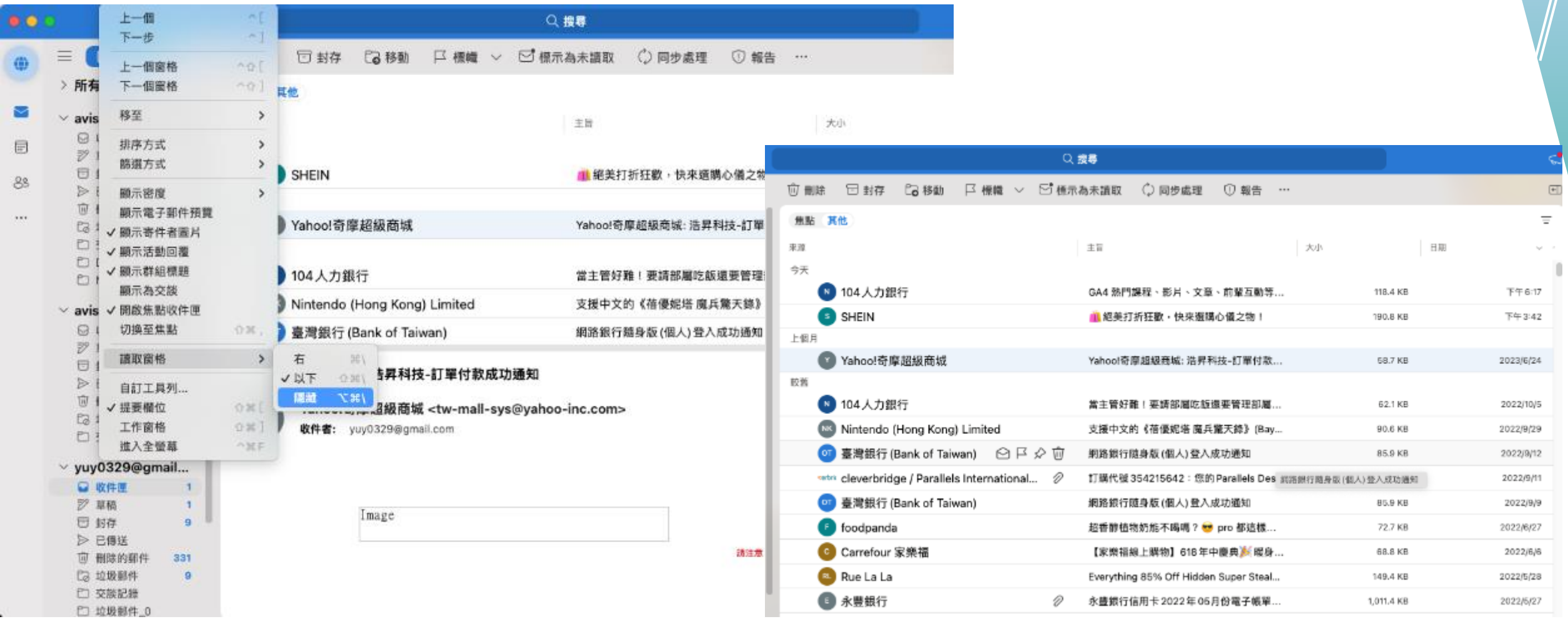
- 為何我會收到這封郵件?
  - 審慎查證寄件來源及寄件者。
  - 不明郵件應立即刪除。
- 我是否應該開啟這封郵件?
  - 確認郵件主旨是否與業務工作相關。
  - 確認有沒有威脅利誘的字眼？有沒有詐騙的可能？
- 我是否應該點選這封郵件附檔及連結?
  - 評估不開啟連結或檔案是否有影響。
  - 不直接開啟檔案，另存新檔後再使用相關軟體開啟。
  - 開啟連結或檔案前，確認對應軟體（如：瀏覽器、Office、壓縮軟體）維持最新更新狀態。

電子郵件停看聽-轉信或回信

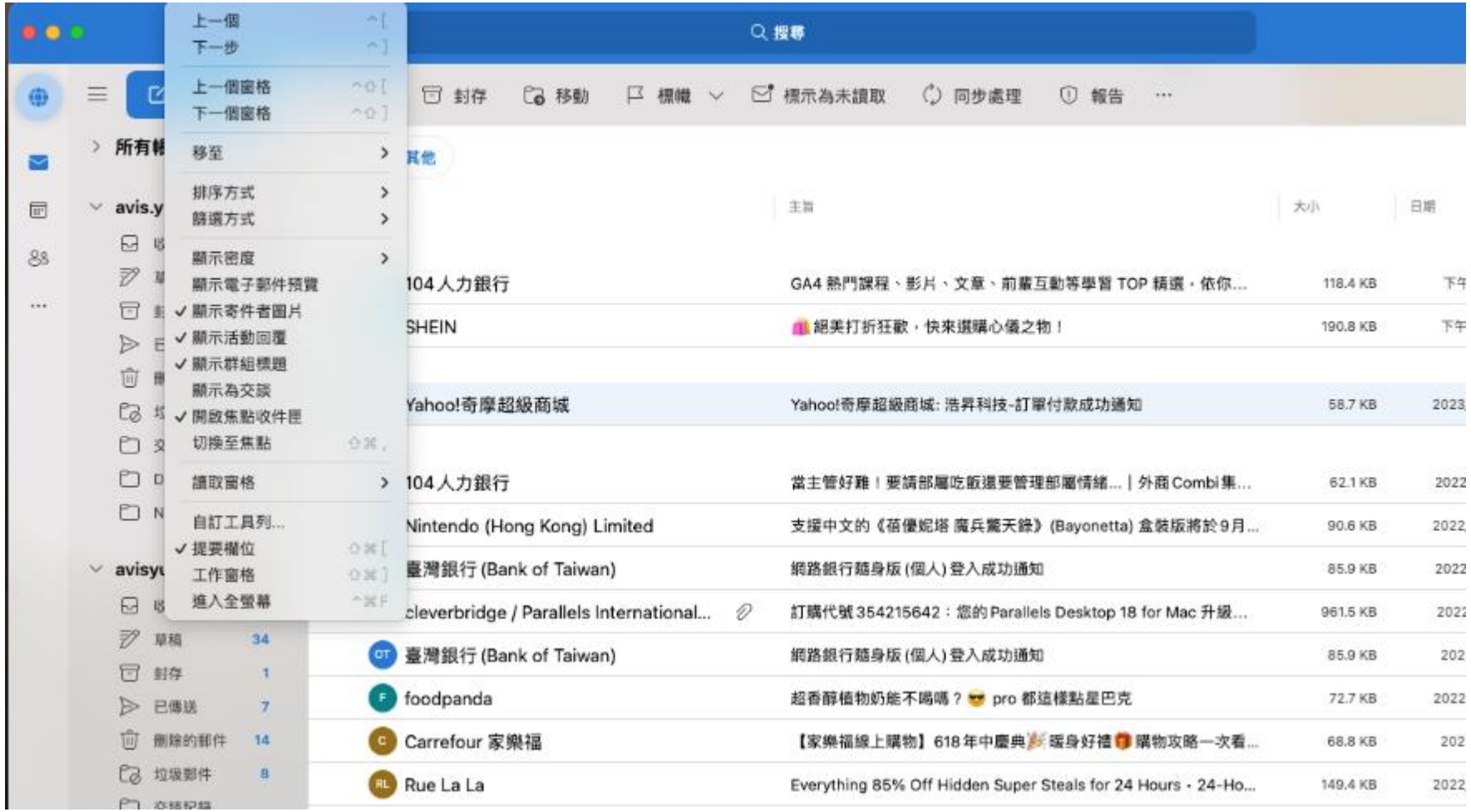
- 我是否應該轉寄這封郵件?
  - 不轉寄未經查證之訊息及不明信件。
  - 轉寄郵件前應先刪除他人郵件地址，避免別人郵件地址傳出。
  - 寄送信件給群體收件者時，應將收件者列在密件副本，以免收件人資訊外洩。
- 我是否應該回覆這封郵件?
  - 審慎查證寄件來源及寄件者。
  - 不輕易填寫個人資料、帳號密碼。

電子郵件設定-關閉自動下載圖片

電子郵件設定-關閉讀取窗格



電子郵件設定-關閉電子郵件預覽



資訊安全案例

系統傳遭中國駭客入侵 國發基金：無資料遭竄改、竊取

2021/07/23 15:25

〔記者巫其倫／台北報導〕有媒體指出，國發基金的創業投資電腦系統，日前遭中國駭客惡意入侵，發生未經授權存取事件。對於此說，國發基金今天強調，6月28日接獲通報後，已立即阻斷不當連線並採取緊急處理措施，另通報資安事件相關單位，同步全面清消且補強防護，初步盤點並未有資料遭竄改或竊取情事。

媒體報導指出，負責國內產業新創與公司轉型的行政院國家發展基金的創業投資電腦系統，上月底遭到大陸駭客惡意入侵，導致系統主機遭植入病毒程式，恐已導致系統內投資企業與融資業務、個人資料嚴重外洩。

國發基金系統日前遭駭，國發基金今天強調，6月28日接獲通報後，已立即阻斷不當連線並採取緊急處理措施。（資料照）

駭客入侵網站偽造接種證書 德國藥局暫停核發

路透社 中文新聞

2021年7月24日 週六 上午12:24 · 1 分鐘 (閱讀時間)

（路透柏林22日電）德國藥劑師協會（DAV）今天表示，在駭客入侵入口網站，偽造COVID-19疫苗接種證書後，目前各藥局已停止核發數位證書。德國疫苗接種作業為此遭受最新挫折。

德國民眾在完整接種疫苗後可領取證書，讓他們行動更自由，特別是在旅行方面。相關證明是由各藥局和疫苗中心核發的。

德國藥劑師協會（German Pharmacists' Association，DAV）表示，駭客入侵入口網站，假扮藥局負責人身分，偽造兩種疫苗接種證書。藥師協會已注意到「商務日報」（Handelsblatt）報導的相關情事。

遭駭偷拍私密片外洩　Sandy站出來面對：過程很難熬

2021-07-22 15:33　噓！星聞 綜合報導　讚 0　分享

電玩實況主Sandy珊迪私密片外流，20日發聲明曝光原來她多年前視訊遭駭客入侵，私生活被違法偷拍，近日還被不肖人士上傳影片、轉發，她透過公司聲明已委由律師團隊處理，呼籲大家勿轉傳，否則將觸犯刑事罪責。

今（7/22）日，Sandy再發文，透露事件（駭客入侵）發生約是在7、8年前，當時她才剛開始做實況工作，覺得能將工作與興趣結合是很好的一件事，沒想到卻被駭被偷拍，近日影片還被散佈，對她造成嚴重傷害。

她說道：「我是女生，我選擇站出來面對傷害我的人以及各種含義騷擾的人，不管是散播者、轉傳、私訊騷擾、留言騷擾、文字騷擾。律師團隊跟我們都有持續截圖，蒐集證據，絕不姑息。」

駭客入侵大量住家網路攝影機　出浴哺乳更衣房事全上網賣

付費加入群組「影片每周更新」　多達4千組免費試看

為了居家安全，現在許多民眾會在家裡安裝網路攝影機(IP Camera)，但進步的科技卻可能嚴重傷害了個人隱私。新加坡爆發一起嚴重的資安事件，有駭客在聊天群組宣稱，已入侵當地多個住家的網路攝影機，民眾在家中更衣、出浴，甚至房事全都遭到側錄，駭客還提供高達4千組「免費試看」片段與截圖取信民眾，聲稱只要付費加入會員，就可觀看每周更新的內容。

駭到你家！73,000 支監視器遭「合法」偷窺，台灣 155 部影片無料觀賞

2014/11/17

Melissa Ye

偷窺一個人很難，要偷窺很多個人那可是難上加難。但別以為你就能隨意在家光溜溜（除非你身材好，媲美世界第八大奇觀），或者是做一些下流齷齪骯髒的事情，因為你做的一切都在別人的眼裡！

有家網站 收集了超過 73,000 支攝影機的錄影畫面 。這家網站並沒有刻意盜入這些人的攝影機，而是因為從一剛開始，這些人就沒有更改攝影機的初始密碼。這網站的目的，到底是想提醒大眾個人的安全問題，還是其實是想從偷窺癖者那邊謀取利益呢？還是，兩者都有？

Live cameras

Live camera in Inazawa, Japan

Live camera in KHARKIV, Ukraine

Live camera in Imola, Italy

Live camera in Tokyo, Japan

Live camera in Tokyo, Japan

Live camera in Macau, Macao

http://www.insecam.org/en/

台南

Live camera in Tainan, Taiwan, Province Of

Live camera in Tainan, Taiwan, Province Of

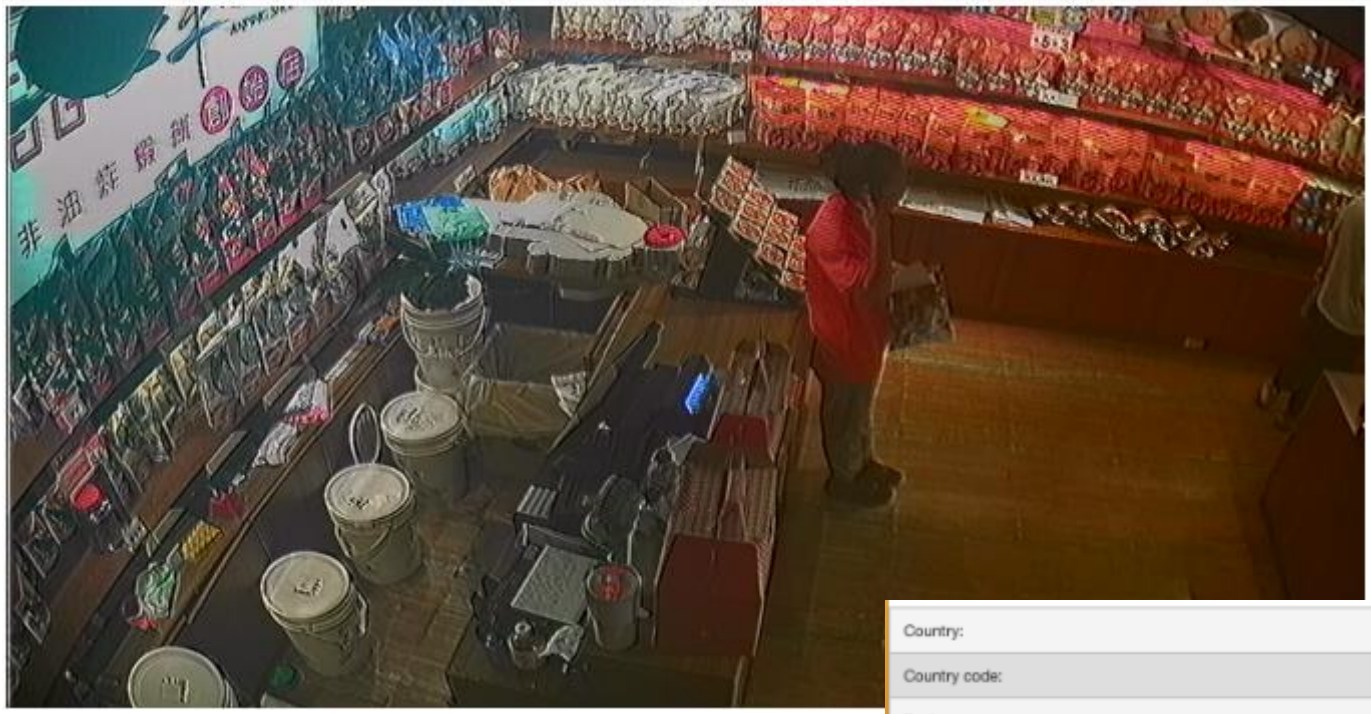
Live camera in Tainan, Taiwan, Province Of

Live camera in Tainan, Taiwan, Province Of

Live camera in Tainan, Taiwan, Province Of

Live camera in Tainan, Taiwan, Province Of

台南安平



Country:	Taiwan, Province Of
Country code:	TW
Region:	Tainan
City:	Tainan
Latitude:	22.990830
Longitude:	120.213330
ZIP:	701
Timezone:	+08:00
Manufacturer:	Hi3516

高雄新興區

你還覺得你家的WebCam安全嗎？

驚傳遭駭客勒索7千萬美元？台積電回應了

16:20 2023-06-30 | 中時新聞網 | 吳美穎

台積電否認遭駭客入侵，而是其供應商擎昊科技被駭。（示意圖/達志影像/shutterstock）

據外媒報導，惡名昭彰的LockBit勒索軟體組織，屢屢駭入各大科技公司勒索巨資，這回鎖定全球晶圓代工大廠台積電，傳出勒索7000萬美元（約台幣21.7億元），並要求8月6日前付款。對此，台積電澄清沒這回事，而是台積電供應商擎昊科技被駭。

自由時報報導，據了解台積電供應商擎昊科技於2023年6月29日上午，發現公司內部特定測試環境中，遭受外部團體的網路攻擊，並擷取相關資訊。擎昊科技表示，已通知客戶台積電，除了對此次資安事件受影響的客戶致歉，也將進行排查、強化資安防護。

每支付一筆贖金等於資助勒索病毒集團未來的 9 次攻擊

2023 / 03 / 08 - 編輯部

新增至最愛文章

趨勢科技指出雖然僅有 10% 的勒索病毒受害者會支付贖金，但這麼做等於讓更多其他企業受害。

趨勢科技威脅情報副總裁 Jon Clay 表示：「勒索病毒是今日企業及政府面臨的一項重大網路資安威脅，而且它還在持續演變，這正是為何我們需要更準確的資料導向方法來為勒索病毒相關的風險建立模型。這份新的研究旨在協助 IT 決策者更了解其曝險狀況，並提供政策制定者一些所需資訊來擬定更有效、更具影響力的策略。」

趨勢科技主要發現：

- 那些同意支付的 10% 受害者通常很快就付款，而且在往後的每一次事件當中所支付的贖金也會越來越高。
- 風險並不是固定的，而是會隨著地區、產業及企業機構大小而異。
- 有些產業及國家的受害者支付的金額比別人高，這意味著其同行也更容易遭到攻擊。
- 支付贖金通常只會拉高事件的整體成本，能獲得的好處不多。
- 勒索病毒集團在1月、7月和8 月謀取獲利的活動較少，因此這段時間是企業重建基礎架構、針對未來威脅預做準備的良好時機。

趨勢科技指出，資安界若能優先強化攻擊前期的防護、持續深入分析勒索病毒的生態系、將心力聚焦於降低支付贖金的受害者比例，將有助於削弱勒索病毒的獲利能力。

惡意程式

病毒

病毒通常以附件的形式出現在裝載有病毒的電子郵件中，或作為執行惡意行為的惡意軟體的一部分。一旦受害者開啟檔案，裝置就會被感染。

蠕蟲

蠕蟲病毒具有從一台機器複製到另一台機器的能力，通常是利用軟體或作業系統中的某種安全漏洞，不需要使用者進行互動即能實現。

勒索軟體

勒索軟體是最有利可圖的一種，也是最受網路罪犯歡迎的惡意軟體之一。 這種惡意軟體會自動安裝到受害者的電腦上，加密他們的檔案，然後索要贖金 (通常是比特幣)，收到贖金後才會將資料還給使用者。

木馬

特洛伊木馬程式偽裝成無害的應用程式，誘騙使用者下載和使用。 一旦啟動和執行，它們就可以竊取個人資料、破壞裝置、監控活動，甚至發動攻擊。

如何得知自己的設備是否感染惡意軟體？

- 電腦已被惡意軟體入侵的最常見跡象包括：
  - 電腦變慢
  - 瀏覽器重新導向，或網路瀏覽器將用戶帶到不打算造訪的網站
  - 感染警告，經常會請求購買一些東西來進行修復
  - 關閉或啟動電腦時出現問題
  - 頻繁彈出快顯視窗廣告
- 用戶看到的這些常見症狀越多，電腦被惡意軟體感染的可能性就越大。 瀏覽器重新導向和大量聲稱您感染了病毒的快顯視窗警告，是電腦已受到攻擊的最強力指標。

我如何保護自己不被惡意軟體攻擊？

- 保護您的裝置
  - 保持更新作業系統和應用程式。 網路罪犯會在舊的或過時的軟體中尋找漏洞，所以要確保一旦有更新就馬上安裝。
  - 絕不要按快顯視窗中的連結。 按一下左上角的「X」關閉訊息，離開產生該訊息的網站。
  - 限制裝置上的應用程式數量。 只安裝您認為自己需要並會經常使用的應用程式。 如果您不再使用某個應用程式，請解除安裝。
  - 不要將手機借給別人，也不要因為任何原因讓自己的裝置處於自動模式，一定要檢查裝置的設定和應用程式。 如果您的預設設定發生了變化，或者神秘地出現了某個新的應用程式，這可能是安裝了間諜軟體的跡象。

我如何保護自己不被惡意軟體攻擊？

- 謹慎上網
  - 避免按下未知連結。 無論是附在電子郵件、社交網路還是簡訊中，如果一個連結看起來不熟悉，請避而遠之。
  - 有選擇性地造訪網站。 盡量只使用已知和信任的網站，以及使用安全搜尋外掛程式，以避開在不知情的情況下出現的任何惡意網站。
  - 小心那些請求個人資訊的電子郵件。 如果一封電子郵件顯示來自您的銀行，並指示您按下一個連結、重設密碼或存取您的帳戶，請不要按下。直接進入您的網路銀行網站並登入。
  - 避開有風險的網站，例如那些提供免費螢幕保護程式的網站。

我如何保護自己不被惡意軟體攻擊？

- 注意下載和購買其他軟體
  - 只在信譽良好公司的官方網站或零售商店內購買安全性軟體。
  - 堅持使用官方應用程式商店。 雖然官方應用程式商店中也可能有間諜軟體，但它們更多見於推廣非官方應用程式的無名第三方商店。 透過為已破解或刷機的裝置下載應用程式，您會略過內建的安全機制，基本相當於將裝置的資料交給陌生人。
  - 當您在尋找下一個您最愛的應用程式時，確保只下載已通過檢驗的應用程式。 閱讀應用程式評論，只使用官方應用程式商店，如果有可疑的情況出現，請避開。
  - 切勿開啟電子郵件附件，除非您知道它的內容，即使它來自您的朋友或認識的人。

我如何保護自己不被惡意軟體攻擊？

- 定期執行檢查
  - 如果您擔心自己的裝置可能被感染，使用裝置上安裝的安全性軟體執行掃描。
  - 定期檢查您的銀行帳戶和信用報告。

中了勒索病毒該怎麼辦（趨勢科技）

- 懷疑感染勒索病毒緊急處理五步驟
  - **將裝置與網際網路斷開連接**。
    您可關閉裝置的 Wi-Fi 或關閉路由器。
  - 將電腦重新開機進入**安全模式**。
    如此一來，電腦就只會執行最基本的應用程式。請注意，將電腦重新開機進入**安全模式**的步驟隨裝置而異。
  - 檢查看看有沒有任何可疑的應用程式，並將它們移除。
    看到任何您不認得的 (或是最近才安裝的) 應用程式嗎？最好通通移除。
  - **將裝置回復到出廠預設值**。
    最好養成定期備份資料的良好習慣，並建立「還原點」
  - **如果前面的步驟都沒有用，那麼您只剩下一招 (除了尋求專業服務之外)，那就是將系統徹底還原。不過請記住，這樣會刪除全部的個人資料、設定和檔案。**

感染勒索病毒 10 項要訣與禁忌:三不七要（趨勢科技）

以下列出 10 項萬一您不幸遭到勒索病毒攻擊時，您該做及不該做的事。

⛔**1.**切勿支付贖金。支付贖金只會變相鼓勵這類攻擊，而且無法保證您能救回檔案。

⛔**2.**小心不要將公司的智慧財產暴露在外以免違反公司規定。這不僅違反職業道德，您可能還會被告上法院。

⛔**3.** 當您在回覆電子郵件、不請自來的電話、簡訊或即時訊息時，切勿提供個人資訊。

✅**4.**採用一套防毒軟體。不過很重要的是一點是要確定它來自信譽優良的廠商，因為網路上有很多假冒軟體**本身就是惡意程式！**

✅**5.**在您的郵件伺服器上安裝一套內容掃描、過濾軟體。所有內送郵件都應經過掃描來過濾掉已知的威脅。

✅**6.**確定所有系統和軟體都隨時保持更新並安裝所有**相關的修補**。

✅**7.**當您出差時，請告知公司的 IT 部門，尤其告知您將會使用公共 Wi-Fi 網路，並且務必學會如何連上公司的**虛擬私人網路** (VPN)。

✅**8.**從可信賴的備份資料將被加密的檔案還原。

✅**9.**仔細閱讀您公司的**電子郵件使用政策**。萬一您不確定某封**電子郵件是否合法**，請聯絡您的 IT 部門。

✅**10.**當您將資料備份到**雲端服務**時，請務必先知會 IT 部門，了解一下公司允許的雲端廠商有哪些。

資安法簡介

立法目的及規範對象

- 立法目的

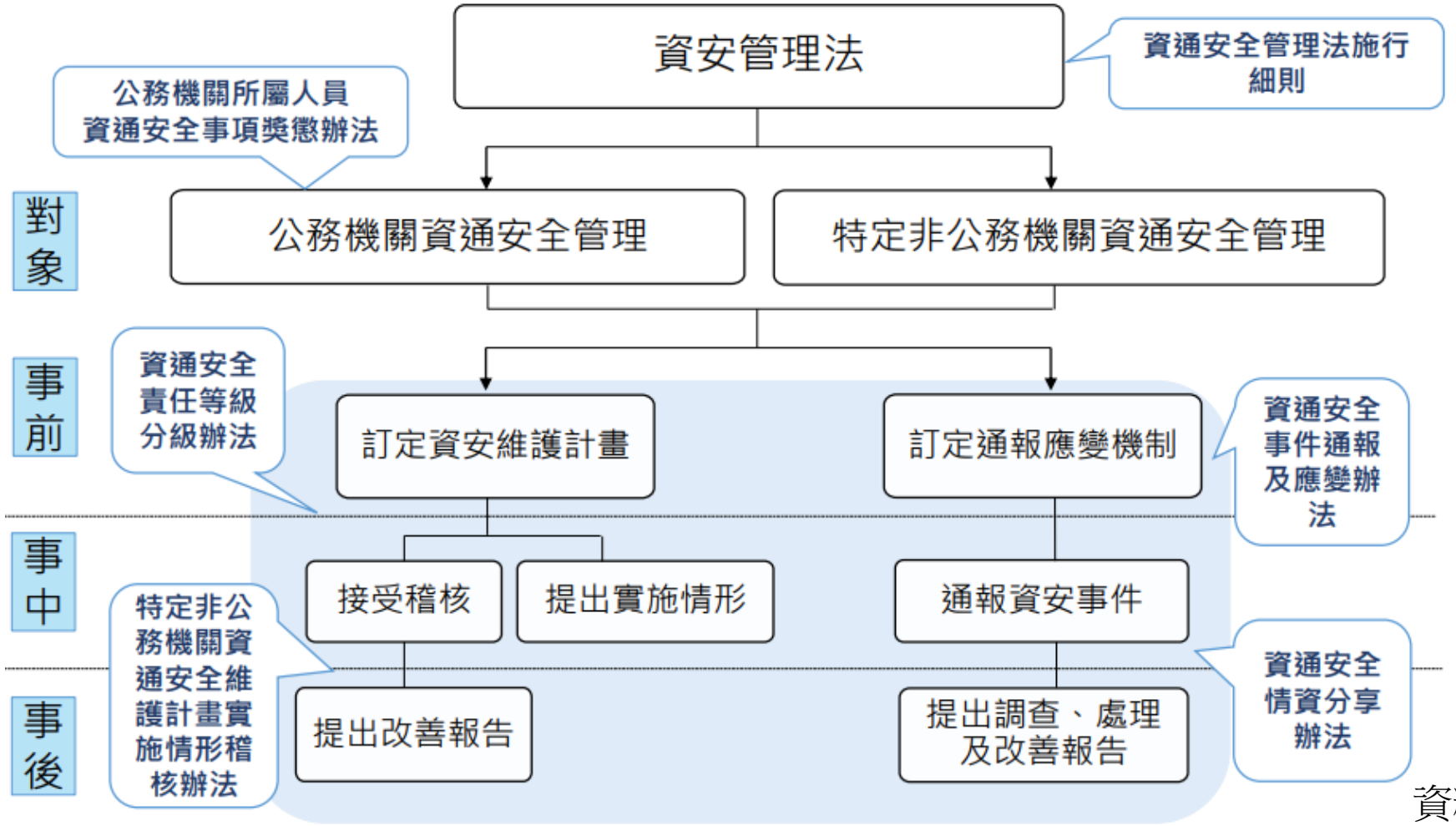
  為積極推動國家資通安全政策，加速建構國家資通安全環境，以保障國家安全，維護社會公共利益。

- 規範對象

  以對人民生活、經濟活動及公眾或國家安全有重大影響者為納管對象。

  - 公務機關：中央與地方機關(構)、公法人。
  - 特定非公務機關：關鍵基礎設施提供者、公營事業、政府捐助之財團法人

資安管理法架構



資料來源：行政院資安處

公務機關資通安全管理規範

- 訂定、修正及實施資通安全維護計畫(第10條)。
- 置資通安全長，由機關副首長或指派適當人員兼任(第11條)。
- 每年向上級或監督機關提出資通安全維護計畫實施情形(第12條)。
- 稽核其所屬或監督機關之資通安全維護計畫實施情形(第13條)。
- 訂定資通安全事件通報及應變機制(第14條)。
- 人員對於機關之資通安全維護績效優良者，應予獎勵(第15條)。

資通安全責任等級應辦事項

- 本校為資通安全責任等級C級單位，依資通安全責任等級分級辦法第11條，應辦理下列事項：
  - 附表五-資通安全責任等級C級之公務機關應辦事項。
  - 自行或委外開發之資通系統應依附表九(資通系統防護需求分級原則)所定資通系統防護需求分級原則完成資通系統分級，並依附表十(資通系統防護基準)所定資通系統防護基準執行控制措施(計7大構面、29類措施)。

附表五　資通安全責任等級C級之公務機關應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	資通系統分級及防護基準		初次受核定或等級變更後之一年內，針對自行或委外開發之資通系統，依附表九完成資通系統分級；其後應每年至少檢視一次資通系統分級妥適性；並應於初次受核定或等級變更後之二年內，完成附表十之控制措施。
	資訊安全管理系統之導入		初次受核定或等級變更後之二年內，全部核心資通系統導入CNS 27001或ISO 27001等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，並持續維持導入。
	資通安全專責人員		初次受核定或等級變更後之一年內，配置一人；須以專職人員配置之。
	內部資通安全稽核		每二年辦理一次。
	業務持續運作演練		全部核心資通系統每二年辦理一次。
技術面	安全性檢測	弱點掃描	全部核心資通系統每二年辦理一次。
		滲透測試	全部核心資通系統每二年辦理一次。
	資通安全健診	網路架構檢視	每二年辦理一次。
		網路惡意活動檢視	
		使用者端電腦惡意活動檢視	
		伺服器主機惡意活動檢視	
		目錄伺服器設定及防火牆連線設定檢視	
	資通安全弱點通報機制		一、 初次受核定或等級變更後之二年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。 二、 本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後二年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。
	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		網路防火牆	
		具有郵件伺服器者，應備電子郵件過濾機制	
認知與訓練	資通安全教育訓練	資通安全專職人員	每人每年至少接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。
		資通安全專職人員以外之資訊人員	每人每二年至少接受三小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受三小時以上之資通安全通識教育訓練。
		一般使用者及主管	每人每年接受三小時以上之資通安全通識教育訓練。
	資通安全專業證照及職能訓練證書		初次受核定或等級變更後之一年內，至少一名資通安全專職人員，分別持有證照及證書各一張以上，並持續維持證照及證書之有效性。

備註：

一、資通系統之性質為共用性系統者，由該資通系統之主責設置、維護或開發機關判斷是否屬於核心資通系統。

二、資通安全專職人員，指應全職執行資通安全業務者。

三、公務機關辦理本表「資通安全健診」時，除依本表所定項目、內容及時限執行外，亦得採取經主管機關認可之其他具有同等或以上效用之措施。

四、資通安全弱點通報機制，指結合資訊資產管理與弱點管理，掌握整體風險情勢，並協助機關落實本法有關資產盤點及風險評估應辦事項之作業。

五、資通安全專業證照，指由主管機關認可之國內外發證機關（構）所核發之資通安全證照。

附表九 資通系統防護需求分級原則

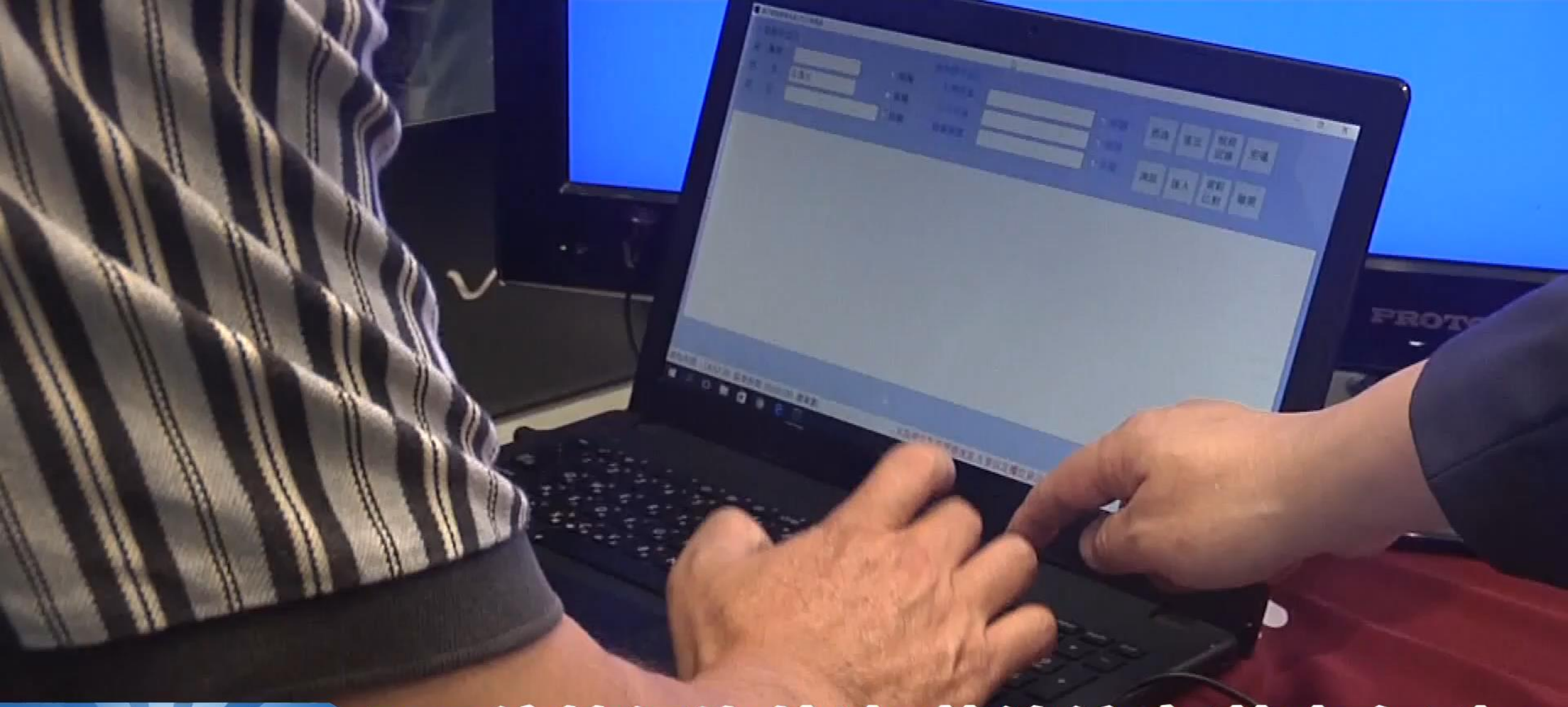
防護需求等級 / 構面	高	中	普
機密性	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生有限之影響。
完整性	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生有限之影響。
可用性	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生有限之影響。
法律遵循性	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關所屬人員負刑事責任。	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關或其所屬人員受行政罰、懲戒或懲處。	其他資通系統設置或運作於法令有相關規範之情形。

備註：資通系統之防護需求等級，以與該系統相關之機密性、完整性、可用性及法律遵循性構面中，任一構面之防護需求等級之最高者定之。

附表十 資通系統防護基準

系統防護需求分級 / 控制措施 構面	措施內容	高	中	普
存取控制	帳號管理	一、機關應定義各系統之閒置時間或可使用期限與資通系統之使用情況及條件。 二、逾越機關所許可之閒置時間或可使用期限時，系統應自動將使用者登出。 三、應依機關規定之情況及條件，使用資通系統。 四、監控資通系統帳號，如發現帳號違常使用時回報管理者。 五、等級「中」之所有控制措施。	一、已逾期之臨時或緊急帳號應刪除或禁用。 二、資通系統閒置帳號應禁用。 三、定期審核資通系統帳號之申請、建立、修改、啟用、停用及刪除。 四、等級「普」之所有控制措施。	建立帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。
	最小權限	採最小權限原則，僅允許使用者（或代表使用者行為之程序）依機關任務及業務功能，完成指派任務所需之授權存取。		無要求。
	遠端存取	一、遠端存取之來源應為機關已預先定義及管理之存取控制點。 二、等級「普」之所有控制措施。		一、對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化。 二、使用者之權限檢查作業應於伺服器端完成。 三、應監控遠端存取

個資洩漏案例



1.7億筆個資外洩 蔡總統.郭董也在列

中天快點TV

台北

跨境網購留意 買3C商品恐個資外洩

娛樂要聞

- 五月天歌迷落寞 世足終戰播倔強
- 僅暖場空檔播出 電視根本沒轉播

⚠高溫黃燈 竹縣

現在溫度 宜蘭 28.5℃

IoT玩具外洩500萬筆兒童資料，香港商偉易達遭罰65萬美元

美國聯邦貿易委員會認為偉易達透過連網電子玩具及搭配App，在未經用戶同意下擅自蒐集兒童與家長資料，且未妥善保護資料，使駭客輕易竊取500萬筆資料，罰款65萬美元。

文/ 李建興 | 2019 01 11 報導

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Contact | Stay Connected | Privacy Policy | FTC en español

Search

ABOUT THE FTC | NEWS & EVENTS | ENFORCEMENT | POLICY | TIPS & ADVICE | I WOULD LIKE TO...

Home » News & Events » Press Releases » Electronic Toy Maker VTech Settles FTC Allegations That it Violated Children's Privacy Law and the FTC Act

Electronic Toy Maker VTech Settles FTC Allegations That it Violated Children's Privacy Law and the FTC Act

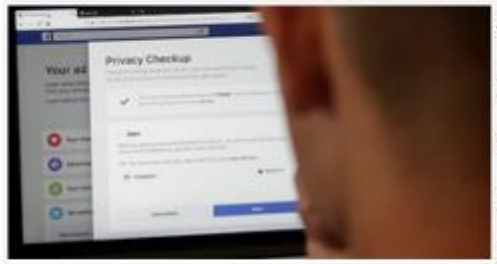
Settlement marks the agency's first children's privacy and security case involving connected toys

EVENTS CALENDAR

In English

臉書CEO祖克伯：雖然我們洩漏了8700萬筆個資，但沒有人是完美的，Facebook還是我來管最好

janus 發表於 2018年4月08日 10:00 | 收藏此文



儘管近來Facebook的爭議不斷，祖克伯可以說是四面楚歌，不過，顯然他依然覺得只有他是Facebook的救世主。他在針對媒體的劍橋分析事件中說明，根據臉書的調查，被劍橋分析收集及使用個人資料的用戶人數，達8700萬人，比原先估計的5000萬，多了3700萬人。不過，他覺得自己依然是Facebook最適合的領導人。

祖克伯還另外自爆了FB的另外一個漏洞，那就是在調查中他們發現，用戶可以透過輸入某人的Email或電話號碼，就可以取得這人在FB的公開資料，不過他表示他們已經刪除了這項功能。

《科技》公務機關個資頻外洩，政院：均啟動資安查核檢討

財經

A A A 友善列印

Facebook Google+ Twitter Weibo

20180717 20:31
豪宅市場回溫？帝寶名媛戶又喊賣 1年加價6200萬

20180717 20:17
境外電商營業人 明年起要開發票

20180717 20:09
SROI公益投資 有助企業社會資本

20180717 20:01
壽險網路投保保費上半年成長8倍 富邦奪雙冠

2017年03月31日 08:18 時報資訊 記者林資傑 / 台北報導

消基會昨（30）日召開記者會指出，公務機關近一年來已發生4起重大資安事件，外洩個資筆數高達13萬筆。行政院資通安全處對此表示，近期政府機關發生重大資安事件，均已立即啟動專案資安查核，進行事故檢討。

消基會指出，包括中華郵政「郵政商城」、勞動部「台灣就業通」、北市資訊局「薪資發放管理系統」及外交部「出國登錄系統」，近一年來接連傳出遭駭洩漏個資，分別達約1.7萬、3.4萬、7萬、1.5萬筆，呼籲應將資安問題納入檢調打擊犯罪專案計畫的執行範圍。

如何竊取個資

駭客釣魚竊個資案 木馬網站 真假只差一點

2007-02-08

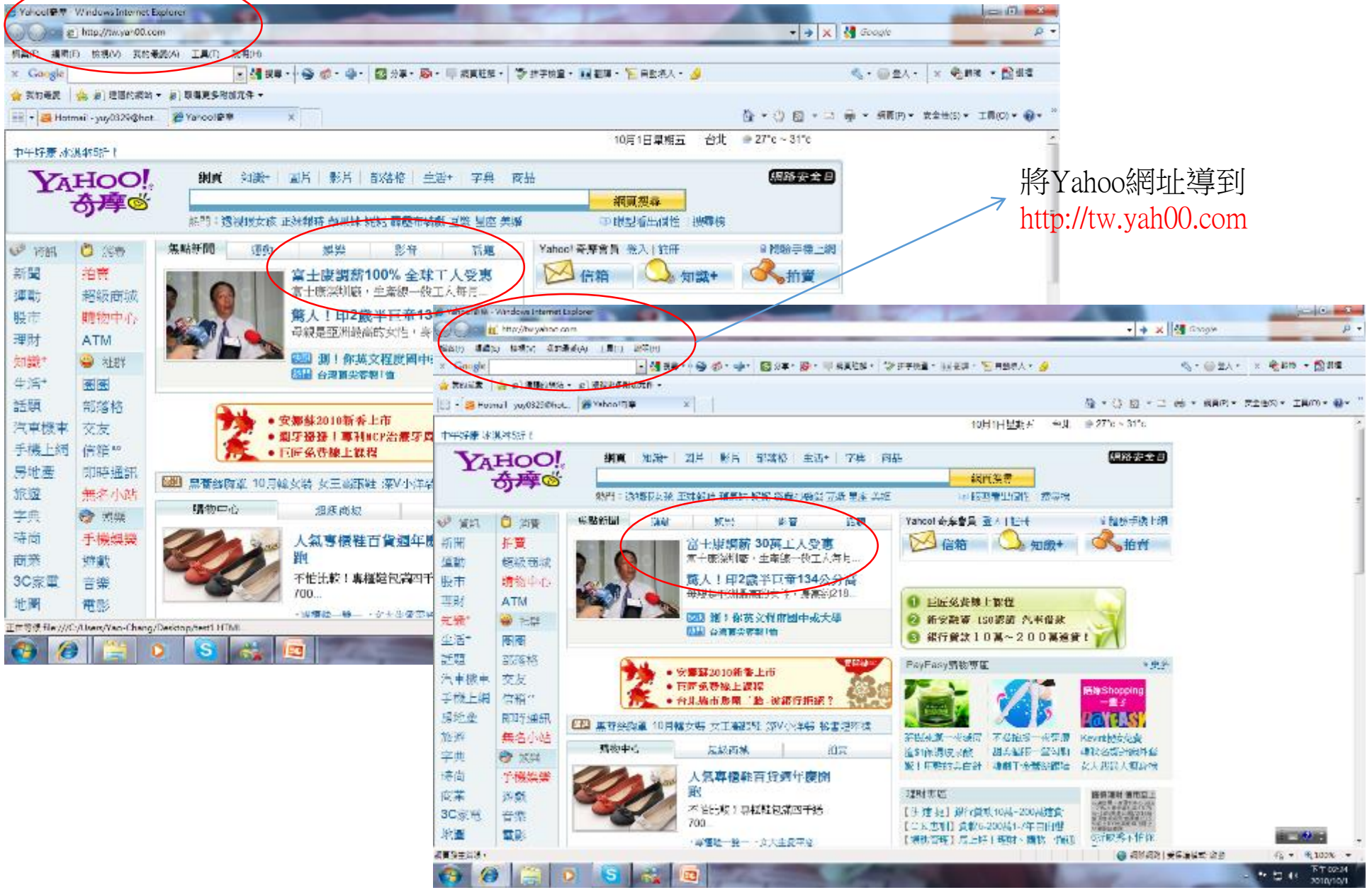
記者黃敦硯 / 特稿

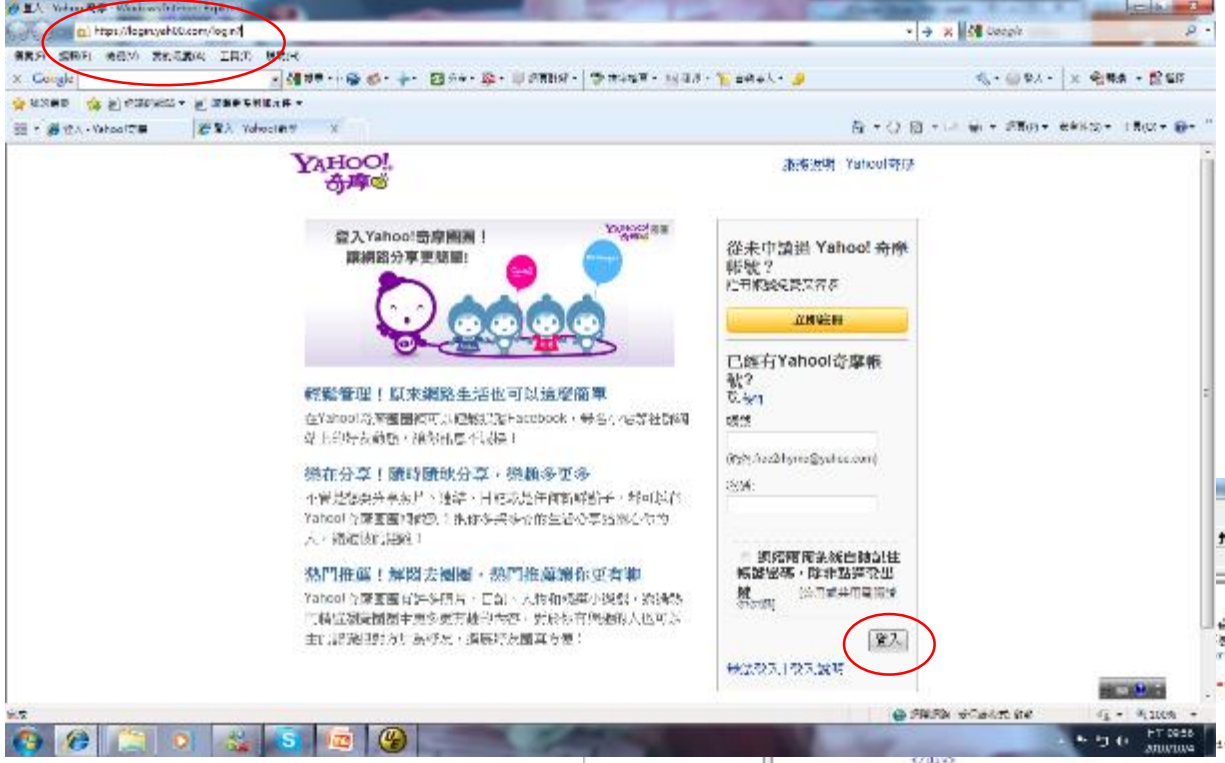
刑事局追查兩岸駭客詐騙集團，發現歹徒是以變種的「網路釣魚」手法取得民眾個人資料，雖然同為架設冒牌網站，利用網友不察而誤連結，但新型的釣魚網站不像過去只竊取被害人的帳號、密碼，而會運用時下相當流行的關鍵字搜尋功能，趁機植入木馬程式，直接把整台電腦的資料偷光光。

更厲害的是，當駭客將木馬植入後，會自動連回「正牌」網站，操作一切如常，民眾根本難以察覺異樣，但已暗暗執行駭客夾藏的木馬。

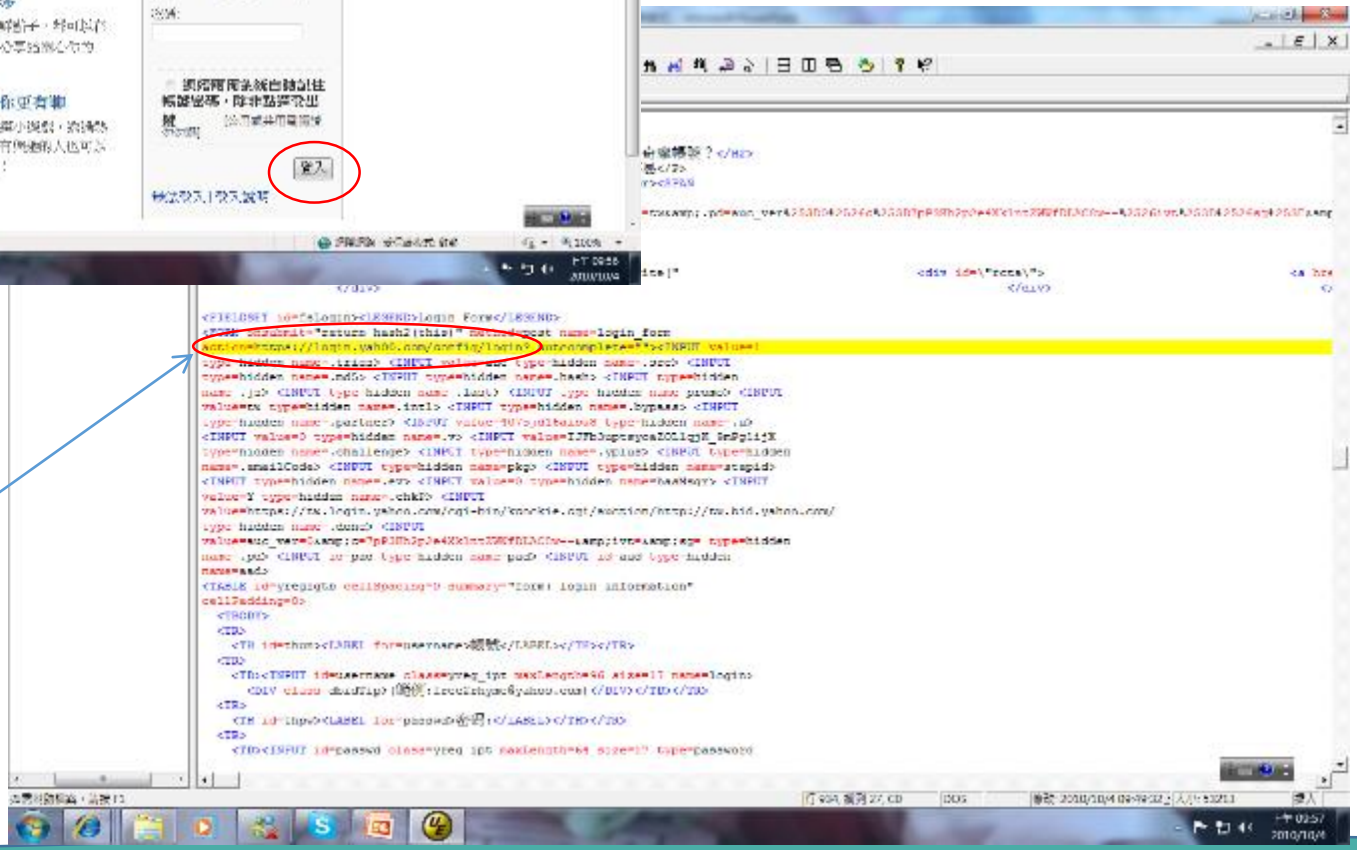
所謂的「釣魚網站」是指，駭客設計一個與正牌網站很像的網頁，讓網友一時不察而誤連結進入，並輸入自己的帳號、密碼，駭客再暗中偷走資料，可是駭客詐騙集團要的不只是帳號、密碼，而是要電腦裡全部的資料。

1、l n、h 網友難辨


將Yahoo網址導到
http://tw.yah00.com



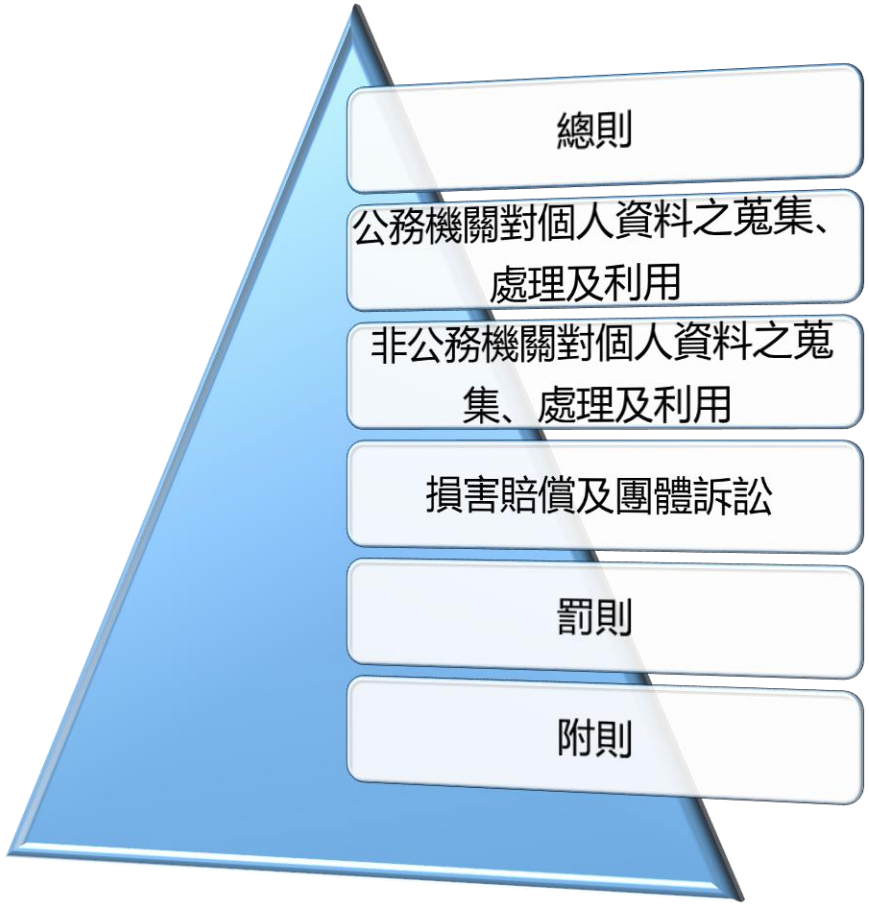
登入位址已更改成
https://login.yah00.com/login?



個資法簡介

個人資料保護法及施行細則

- 個人資料保護法（104年12月30日）
  - 六章
  - 56條
- 個人資料保護法施行細則（105年3月2日）
  - 33條



何謂個人資料

個人資料: （個資法第一章第二條）
1. 指自然人之姓名
2. 出生年月日
3. 國民身分證統一編號
4. 護 照號碼
5. 特徵
6. 指紋
7. 婚姻
8. 家庭
9. 教育
10. 職業
11. 病歷
12. 醫療
13. 基因
14. 性生活
15. 健康檢查
16. 犯罪前科
17. 聯絡方式
18. 財務情況
19. 社會活動
20. 及其他得以直接或間接方式識別該個人之資料。

個資法第一章第六條)
1. 病歷
2. 醫療
3. 基因
4. 性生活
5. 健康檢查
6. 犯罪前科

間接方式識別： （施行細則第三條）
僅以該資料不能直接識別，須與其他資料對照、組合、連結等，始能 識別該特定之個人。

個人資料檔案

- 個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式 檢索、整理之個人資料之集合。
  - 施行細則第5條：個人資料檔案，包括備份檔案。

蒐集

- 蒐集：指以任何方式取得個人資料。

第 8 條
公務機關或非公務機關依第十五條或第十九條規定向**當事人蒐集個人資料時，應明確告知**當事人下列事項：
一、公務機關或非公務機關名稱。
二、蒐集之目的。
三、個人資料之類別。
四、個人資料利用之期間、地區、對象及方式。
五、當事人依第三條規定得行使之權利及方式。
六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。

→ 直接取得

第 9 條
公務機關或非公務機關依第十五條或第十九條規定蒐集非由當事人提供之個人資料，**應於處理或利用前，向當事人告知**個人資料來源及前條第一項第一款至第五款所列事項。

→ 間接取得

處理

- 處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、 編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。
  - **新增文件、建檔案、輸入系統**
  - **編輯檔案、刪除檔案、儲存檔案、複製檔案**
  - **檢索查詢、更正錯誤、製作連結**
  - **內部傳送至別部門/單位**

利用

- 利用：指將蒐集之個人資料為處理以外之使用。
  - 對當事人使用其個資：如使用通訊錄打電話或寄信、E-mail。
  - 揭露第三方：如提供檢調單位調查、提供主管機關備查、提供勞健保給勞健保機構、提供報稅資料給國稅局、稅捐單位。

個資當事人的權利

- 當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：
  - 查詢或請求閱覽。
  - 請求製給複製本。
  - 請求補充或更正。
  - 請求停止蒐集、處理或利用。
  - 請求刪除。

職員

個人資料

人事室

資料建檔

人事薪資系統

出納

查詢人事薪資資料

印領清冊

會辦核銷

主計室

職員

個人資料
（蒐集）

人事室

資料建檔
處理（輸入）

人事薪資系統

查詢人事薪資資料
處理（檢索）

處理（儲存、
刪除）

出納

印領清冊
處理（輸出）

會辦核銷
處理（內部傳送）

處理（儲存、
刪除）

主計室

問答 1

- **私立學校於實施教育之範圍內，為個人資料保護法所稱公務機關或非公務機關？**

個資法問與答

【個資法即時通】私立學校於實施教育之範圍內，為個人資料保護法所稱公務機關或非公務機關？

張貼日期：2013/07/24

答：個資法所定之公務機關，係指依法行使公權力之中央或地方機關或行政法人。因此，公立學校如係各級政府依法令設置實施教育之機構，而具有機關之地位，應屬個資法之公務機關。至於私立學校，雖然由法律在特定範圍內授與行使公權力，惟私立學校在適用個資法時，為避免其割裂適用個資法，並使其有一致性規範，私立學校應屬個資法所稱之非公務機關。

(摘自「法務部102年6月24日法律字第10200571790號書函」-本函全文可於本部全球資訊網點選「法務部主管法規查詢系統」查詢)

問答 2

- **學生校服如繡上姓名、學號是否違反個資法？**

個資法問與答

【個資法即時通】學生校服如繡上姓名、學號是否違反個資法？

張貼日期：2015/03/31

一、按個資法係為規範個人資料之蒐集、處理及利用而設（個資法第1條規定參照）。旨揭疑義係學校要求學生於制服繡上姓名、學號，尚未涉及學校蒐集、處理及利用個人資料，故無個資法之適用，合先陳明。

二、次按教育部訂定之「學校訂定教師輔導與管教學生辦法注意事項」第21點第4項規定：「除前項情形外，有關學生服裝儀容之規定，應以舉辦校內公聽會、說明會或進行全校性問卷調查等方式，廣納學生及家長意見，循民主參與程序訂定，以創造開明、信任之校園文化。」是旨揭疑義係屬學校之教育管理規定是否合法妥適，宜由教育部本諸職權釐清。（摘自「法務部104年1月19日法律字第10403500300號函」-本函全文可於本部全球資訊網點選「法務部主管法規查詢系統」查詢）

問答 3

- **悠遊卡股份有限公司所發行結合各大專院校學生證功能之記名式悠遊卡，就蒐集學生個人資料之方式應如何適用個資法？**

個資法問與答

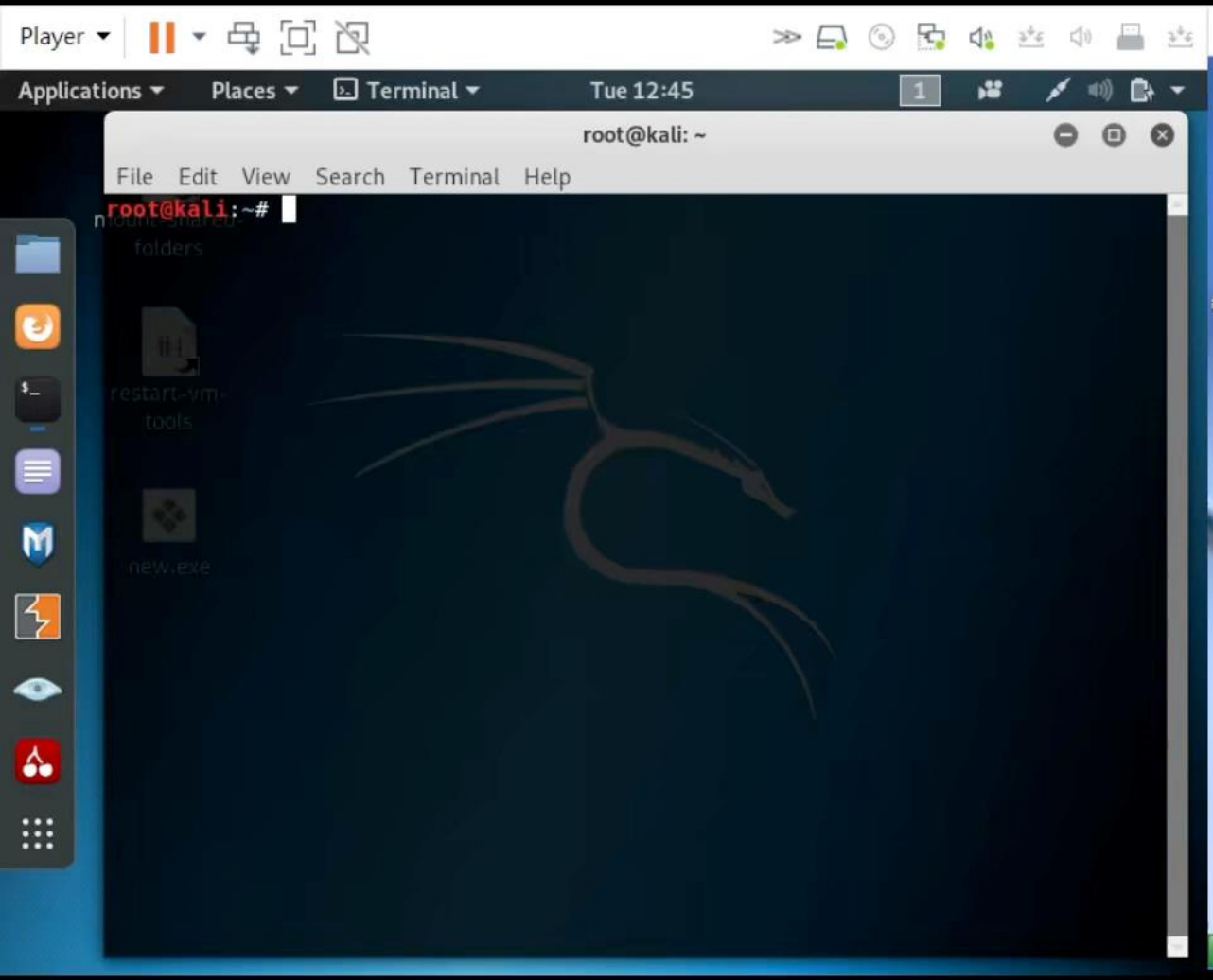
【個資法即時通】悠遊卡股份有限公司所發行結合各大專院校學生證功能之記名式悠遊卡，就蒐集學生個人資料之方式應如何適用個資法？

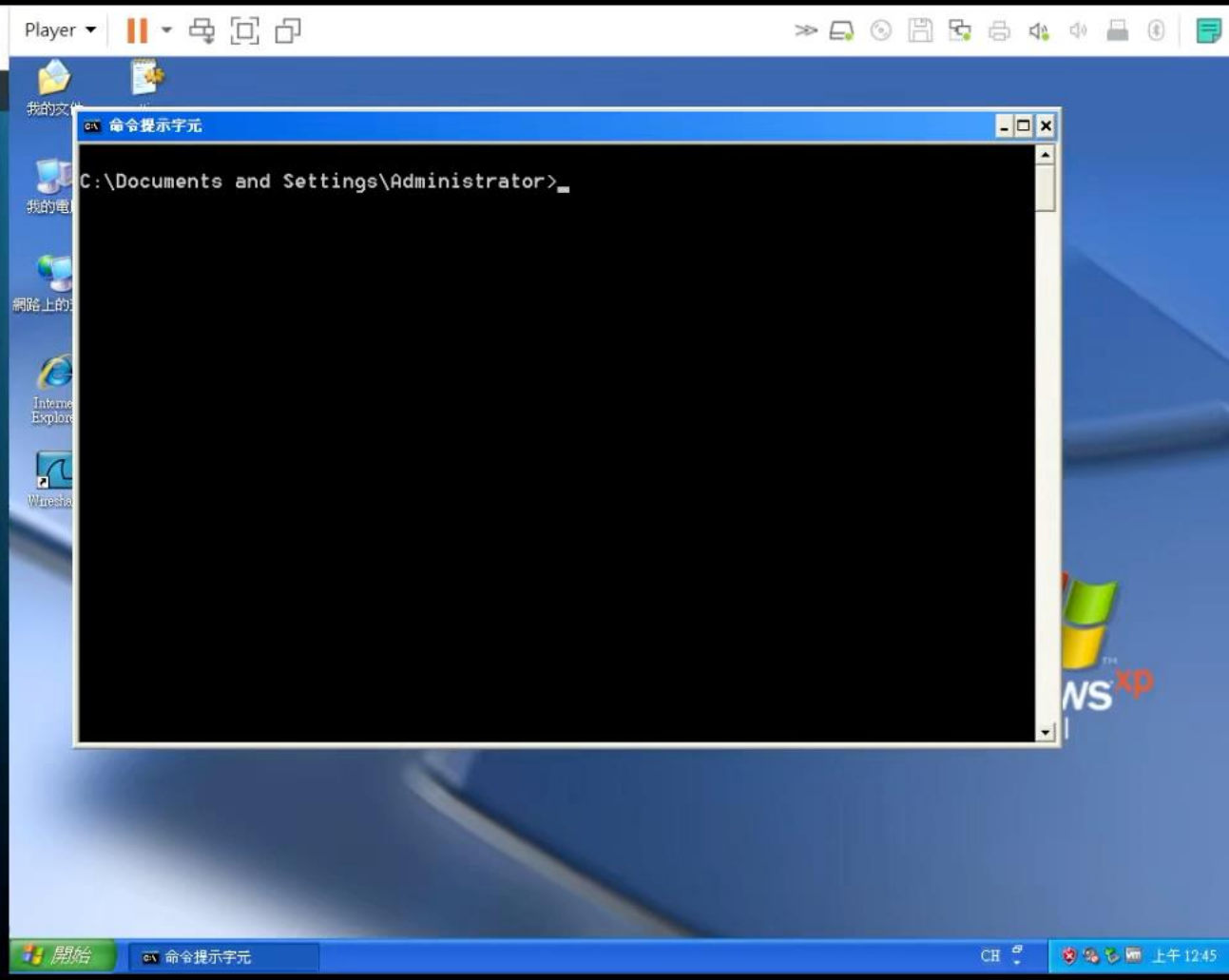
張貼日期：2013/06/10

答：悠遊卡股份有限公司(下稱悠遊卡公司)所發行結合各大專院校學生證功能之記名式悠遊卡（下稱校園卡），悠遊卡公司與學校間訂有校園卡之採購契約，該契約之主體為悠遊卡公司與學校，惟該採購契約僅為提供悠遊卡公司與學生間成立契約關係之平台，學生後續使用校園卡乘坐大眾運輸交通工具或為其他消費行為，甚或票卡遺失時辦理申請掛失及返還餘額等事項，均係直接向悠遊卡公司為之，故有關悠遊卡公司若係依個資法第 19 條第1項第2 款規定而取得學生之個人資料，應係基於與學生間之電子票證定型化契約，而與學校間之採購契約無涉。另學校基於教育行政或學生資料管理之特定目的，蒐集、處理或利用學生之個人資料，包含核發學生證，惟就學生證結合記名式悠遊卡之功能，由學校將學生之個人資料提供予悠遊卡公司，為特定目的外之利用，應區分公立學校或私立學校而分別依個資法第16條但書、第20條第1項但書規定為之。

攻擊者

受害者

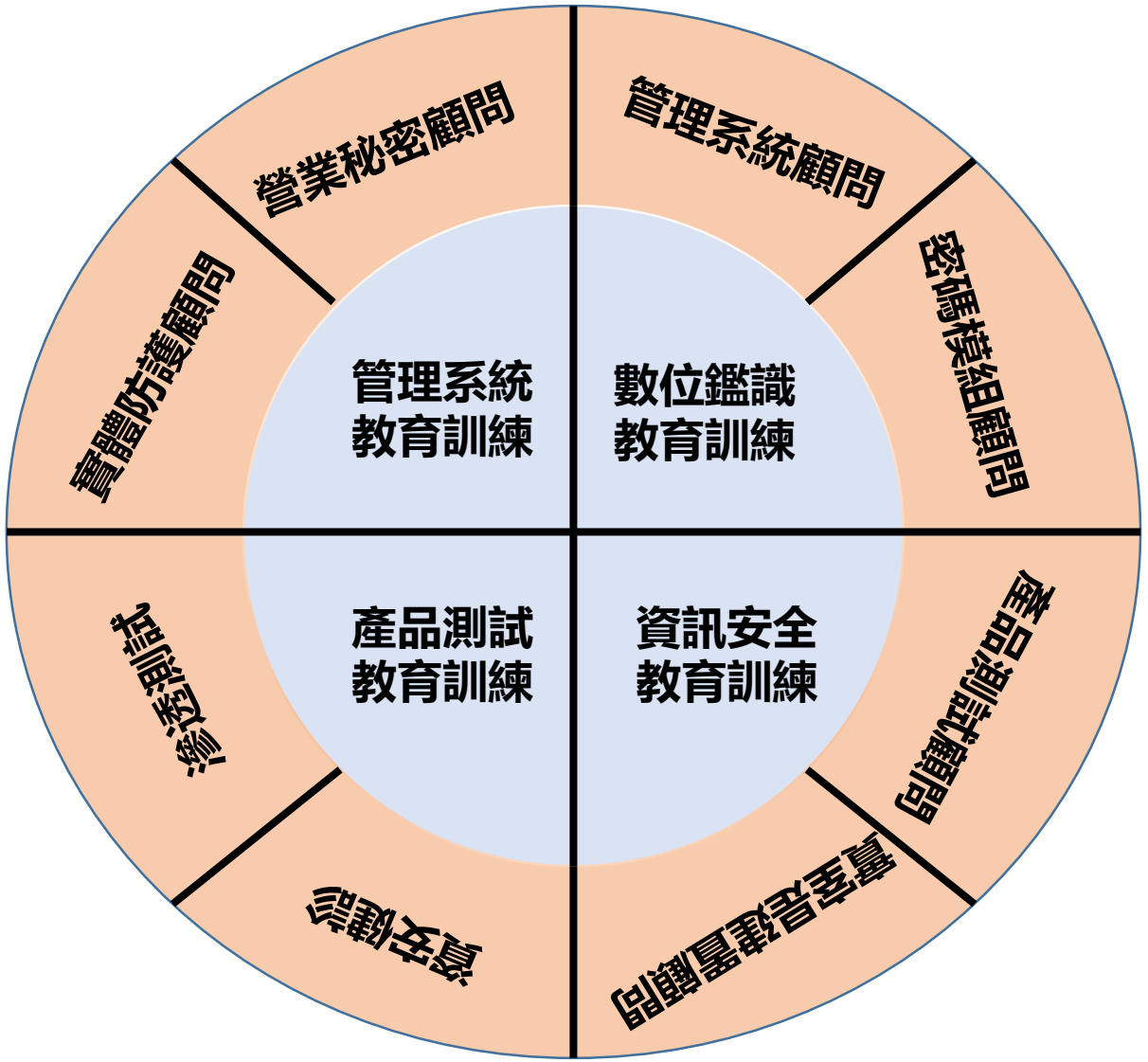




駭客要製作一個能遠端操控被害者電腦的病毒並不困難

關注方的想法及回饋

Q/A


營業秘密顧問
管理系統顧問
密碼模組顧問
實體防護顧問
管理系統
教育訓練
數位鑑識
教育訓練
產品測試
教育訓練
資訊安全
教育訓練
滲透測試
資安健診
實品測試顧問
資安諮詢顧問

優士創造您的資安優勢