公務機密
資訊安全維護

- 非官方的APP不要安裝,才能減少威脅
- 不要使用行動裝置進行重要交易
- 來路不明的簡訊連結要小心

資安時事案例

欠缺資料無法運送包裹 輸入信用卡恐遭盜刷

駭客溜進Microsoft Teams會議以大量散布木馬程式

個人資料保護法

個資法規範的行為與對象

生活中的資安

視覺密碼-迷人的眼「神守護」

數位學習

106年資安動畫金像獎
「童話故事也要慎防詐騙」

欠缺資料無法運送包裹 輸入信用卡恐遭盜刷

民眾日報 2022年2月10日

【記者方筐楠臺北報導】一名住於臺中年約30歲，從事資訊科技業的柯小姐，日前接獲一封 +46開頭的手機簡訊，內容為「欠缺資料，我們無法運送您的包裹」，並附上包裹編號以及短網址。由於柯小姐原本就有網購習慣，便不疑有他點擊簡訊中提供的網址，接著連結到「DHL快遞」的網站，柯小姐按照網站指示，逐步填輸個人姓名、電話、地址等個人資料，並登打信用卡卡號進行網上付款，當時網頁顯示需消費金額為12.47元，柯小姐點擊付款後，便收到銀行通知的OTP驗證碼，其中有標明即將消費歐元(EUR)1,649元，但是柯小姐並未仔細查看，便於該網站輸入驗證碼，等收到銀行通知確認刷卡金額為新臺幣5萬2,767元時，才驚覺狀況有異，立刻撥打DHL官方客服確認，這才知道稍早收到的簡訊、填輸個資的網站全都是假的，自己的信用卡已被詐騙集團盜刷!

165反詐騙諮詢專線統計，今年1月至2月8日，受理民眾報案稱收到有包裹無法運送簡訊，連結至假DHL、FedEx網站而遭詐騙之案件共19件，總受害金額約84萬餘元。經查，此為歹徒透過亂槍打鳥的方式發送簡訊，以包裹正在等待送達、出現問題為由，並附上釣魚短網址誘騙點擊，連結至假冒的快遞網站後，要求輸入姓名、信用卡卡號、有效期限、安全碼等個人資料來支付郵資或手續等費用。若不察完整填輸，個人資料立即遭竊取用以盜刷，俟收到銀行通知消費簡訊提醒，始知遭到詐騙。

針對此類手法，DHL於官網提供詐欺防制意識說明，提供辨別方法，例如簡訊詐騙通常會含有造成混淆的短網址連結，或者發送簡訊電話特殊，例如開頭為+235、+46等，您可截下含有可疑電話和簡訊的螢幕畫面，通報至phishing-dpdhl@dhl.com。FedEx亦於官網提供線上詐騙警示說明，提醒用戶若收到可疑郵件、簡訊，請立即刪除，切勿輸入任何個人資訊。這些快遞公司並不會向客戶傳送不請自來的、要求其提供包裹、請款單、帳號、密碼、個人資訊的電子郵件。

165反詐騙專線提醒您，收到各類資訊、通訊內容時，先保持「零信任」態度，先確認簡訊發送電話、點擊後連結網址是否有被混淆。另外當平時有已知的郵局包裹、郵件運送時，需特別提高警覺，與寄送方保持聯繫，亦不隨便點擊釣魚連結、輸入信用卡資料等個資。萬一誤輸入並送出了信用卡資料時，請立即通知發卡銀行啟動停卡，將損失降至最低。民眾如發現有不明電子郵件、簡訊並帶有可疑網址之顧慮，可撥打165反詐騙專線即時查證，以維自身財產安全。

駭客溜進Microsoft Teams會議 以大量散布木馬程式

資料來源:iThome 文/陳曉莉 | 2022-02-18

透過視訊會議平臺傳送的檔案也有安全風險，資安業者發現近來每月有數千起網路攻擊，是駭客盜取M365憑證混入Microsoft Teams會議及聊天室，散布惡意執行檔給群組成員

資安業者Avanan本周警告，隨著Microsoft Teams愈來愈受歡迎，它已成為駭客鎖定的攻擊目標，駭客藉由溜進Microsoft Teams會議，以大量散布木馬程式，該公司每個月都可看到數千起的相關攻擊。

根據微軟今年1月的估計，Microsoft Teams每月用戶數已達2.7億，然而，同一時間Avanan也觀察到，駭客正積極利用Microsoft Teams散布木馬程式。

駭客是透過各種方法滲透到Teams中，例如先入侵組織的供應鏈或合作夥伴，以竊聽它們之間的對話，或者是危害用來存取Teams的電子郵件帳號，或是藉由網釣攻擊取得使用者的Microsoft 365憑證，接著就以這些身分登入Teams會議，再於會議或聊天中丟出惡意的執行檔。

這些執行檔的名稱很普通，例如其中一例為User Centric，但執行後它會在Windows登錄檔中寫入資料，安裝DLL檔案，並建立捷徑以讓該程式能夠自我管理，進而控制受害者電腦。

由於Teams屬於團隊協作平臺，因此當駭客得以溜進Teams會議或聊天室中時，將可一次感染眾多的受害者。

Avanan指出，由於Microsoft Teams屬於新興的平臺，目前防禦機制有限，再加上大多數的使用者尚未經過相關的資安洗禮，而讓駭客更容易得手。例如使用者可能對電子郵件的安全性較有感，卻相對信任Microsoft Teams；或者是從未懷疑那些進入Microsoft Teams的同事，甚至是執行長等高階主管，可能是駭客假冒的；也更容易於Microsoft Teams中分享各種機密文件。

最近的攻擊行動也讓Avanan提醒使用者，應該對這些協作平臺更有安全意識，例如應該檢查下載的所有內容，針對所有商業通訊部署安全機制，組織亦應鼓勵使用者檢舉可疑的文件。

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

一組長度 4 位數的密碼，可以在幾分鐘之內破解，但長度 8 位數以上的組合，就可能要花上一個月的時間才能破解,。

如何讓系統知道我是誰

電影或電視中，我們常可見到要進入管制區或要存取機密訊息時，都一定會有一套身分鑑定的程序，確認使用者的身分之後再來決定其權限。而在今日不管使用何種安全系統，第一步也都是身分鑑定，我們要讓系統知道我是誰？我是否被允許登入系統？我擁有哪些權利？系統一收到我們所輸入的訊息後，就可以知道我們是誰並且清楚我們是否有權執行哪些指令或閱讀哪些檔案。

就目前一般較為廣泛應用的系統而言，身分鑑定主要有以下三項：你所記得的東西、你的特徵、或你所持有的東西。這些大致上可對應到「密碼」（Password）、「生物測定學」（Biometrics）、及「信物」（Token）。

圖 1 傳統的身分鑑定方法是使用個人帳號與密碼

身分鑑定方法1-密碼

先來談「密碼」，身分鑑定的傳統方法是使用個人帳號與密碼，例如我們經常使用網頁進入 Email 的系統，或者提款時所輸入的密碼、在網路上購物時所輸入的個人帳號與密碼，如圖 1 所示。密碼登入方式是使用電腦系統中存有一個使用者代圖 1 傳統的身分鑑定方法是使用個人帳號與密碼號及對應的密碼清單資料庫。因此若在使用者輸入時有任一項不符的話就會被系統拒絕，這是最簡單也最易被實作的方法。然而使用者代號及密碼並不如我們想像中可靠，因為以密碼作為身分鑑定是假設使用者會選擇諸如「E1Bk%Y!o9」等無意義的文數字組合作為密碼，而非「1369」、「TWNSB」、「MJIB」等有意義且方便記憶的組合作為密碼。

密碼是否為「無意義」的文數字組合與其「長度」等兩大元素是決定其是否有效的關鍵要點。例如：一組長度 4 位數的密碼，可以在幾分鐘之內破解，但長度 8位數以上的組合，就可能要花上一個月的時間來破解，因此，選擇不當的密碼，就易於被攻擊者攻破。然而，對使用者而言，

要能記憶多組不同的密碼也是一大挑戰，不經意會造成管理上的負擔。

身分鑑定方法 2—生物特徵

生物特徵源自於「生物測定學」，係一種依據使用者獨有的生理或行為特徵為基礎所建立的資料作為識別與認證基準的方法。目前發展中的生物特徵辨識技術包括指紋、眼睛虹膜（Iris）、視網膜（Retina）、脫氧核醣核酸（DNA）、掌形（Hand Geometry）、聲紋、手寫簽字、鍵盤敲打頻率、臉型、脣型等。其中，指紋辨識技術發展最早且較成熟，是現階段較具代表性的技術。多年來，「生物測定學」在身分鑑定上的技術越來越好，其優點在於使用者無須攜帶任何東西或是記憶密碼即可達到身分識別與認證的目的；另一優點則是生物特徵難以偽造，製作假指紋與視網膜是相當困難的。然而缺點在於一套完善的生物測定機器相當昂貴，且精確度標準不易測量，精確度提高，系統辨識速度就會減慢；精確度降低，則安全度不夠，此外，使用生物特徵還要面對個資隱私的質疑。

身分鑑定方法 3—信物

第三種即是使用我們所持有的東西，來證明我們的身分，也就是「信物」的概念。例如電視、電影上常見，在古代拿著朝廷的令牌或是尚方寶劍便可代表朝廷行使職權，這令牌或尚方寶劍就是信物的一種。目前最常見的就是利用智慧卡（Smart Card）、IC 卡（Integrated Circuits Card）來作為為信物。如此一來，使用者無須記憶複雜的密碼，遺失了一樣可以補發。但

目前生物特徵辨識包括指紋、眼睛虹膜、DNA、掌形、聲紋、手寫簽字、臉型等多種技術。

是使用此法的缺點一樣是要面臨信物會被竊取、仿冒或是被複製的問題。同時，攻擊者可以針對智慧卡或是 IC 卡來進行破解以取得系統重要的資訊。

在這三種方法中，現今在運用上多是以一、二種來進行身分鑑定。然而，卻還有一個問題難以解決，也就是「內賊」。內部不肖人員可以直接竊取系統資料庫的鑑定比對資訊，使得所屬單位損失慘重。因此，要做出好的安全系統，最好是讓雙方共享祕密資訊，而任一方所擁有的資訊無法讓他推斷出全部的資訊。在這一方面上，目前最具成效的應用之一就是視覺安全！

視覺密碼—迷人的眼「神守護」

視覺密碼（又稱視覺安全）主要是依據人類視覺系統對於影像色差的反應，而賦予影像意義為基礎。例如在進行健康檢查時，檢測色盲所用的卡片，便是以人眼視覺的反應來判斷多個不同色彩的雜點所包含的訊息。**視覺密碼解決了傳統密碼學在解密過程中需要大量複雜的計算過程**，在安全性上，同樣可以確保竊取資料者無法從這些個別的分享影像（或稱為子圖）中，察覺出機密影像的輪廓。

使用視覺密碼方法的優點在於可使得電腦系統與使用者雙方所持有的資訊都是無意義的圖形，唯有在正確的組合之下，才會顯現出有意義的訊息。而這樣的方式會使得有意進行攻擊或入侵者**必須同時取得雙方的資訊方可成功**，藉此得以降低入侵行為的成功率，因此能有效提高系統的安全程度。

視覺密碼**不需要複雜或大量的數學計算，也可以不需要電腦的輔助來完成解讀，只要藉由人類的視覺系統即可直接解讀出機密訊息。**

視覺安全的完美祕密

視覺安全是 1994 年所提出的概念，這種方式並不需要用到任何密碼學的專業知識。視覺安全具有視覺化、操作簡易、高度保密等優點，使得密碼學得以邁向另一個不同的層面，但在作法上仍會產生一些需克服的缺點，例如影像容量的增加、影像對比的下降及影像的清晰度等問題。

在傳統視覺密碼中，為了達到祕密分享的目的，機密影像中的每一個像素（Pixel）都會被擴張成若干個子像素（Sub-pixel），此作用稱為像素擴張（Pixel-expansion），在原始提出的基本觀念裡是將祕密影像中每一像素擴張成 1 × 2 的區塊。若原祕密影像圖的像素值是白色，所分解出的分享圖疊合起來（分享圖 1 + 分享圖 2）會是一黑一白的像素區塊；若原祕密影像圖的像素值是黑色，分

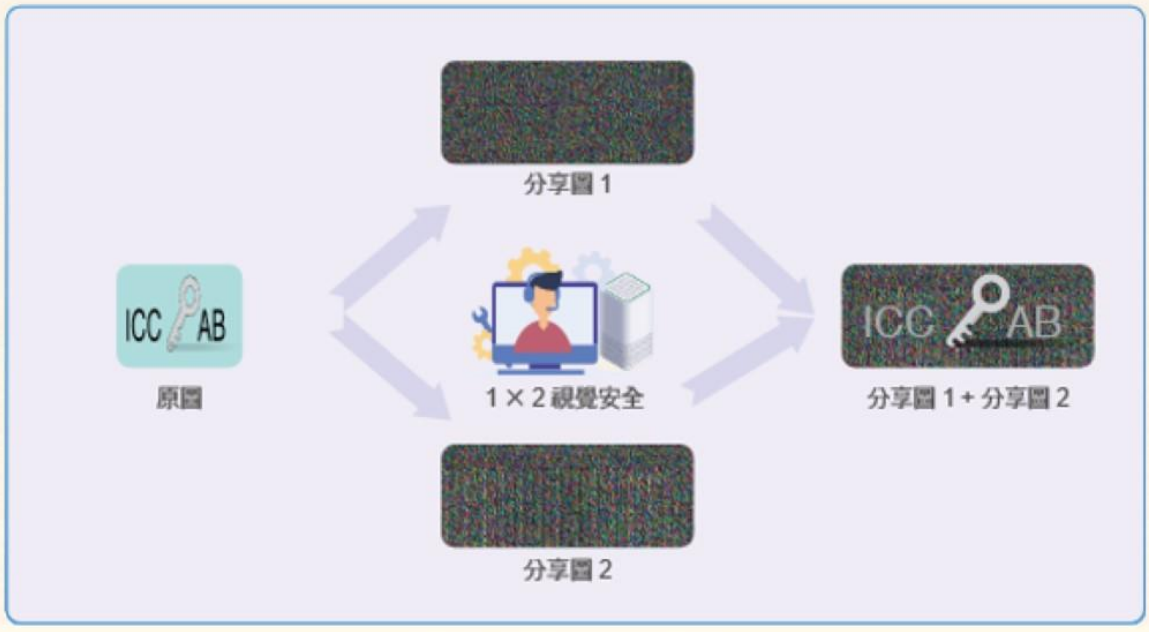

圖 2　視覺安全基本概念

享圖疊合則是二個黑點像素區塊。藉由這種方式，所分解出來的分享圖個別而言會是無意義的影像，但疊合起來的結果，以人類的視覺系統觀察，卻可還原成原來的祕密影像，如圖 2 所示。而其所呈現的效果將使祕密影像有拉長的視覺效果，形成不等比例之擴張。

視覺安全最初的設計是在黑白的二元影像上，主要是將擁有祕密資訊的機密影像分解成 2 張分享影像。（0）表示白色、（1）表示黑色，如果機密影像的像素點為白色，可分為兩張分享影像。將原機密影像每個像素點擴張為兩倍成為分享影像，也就是分享圖 1 為兩倍像素點（1，0）或（0，1），分享圖 2 為兩倍像素點（1，0）或（0，1）。若點為黑色的話，分享圖 1 為（1，0）或（0，1），分享圖 2 為兩倍像素點（0，1）或（1，0）。依序將整張機密影像分解成兩張分享圖，其表現出的方法就如圖 3 所示。

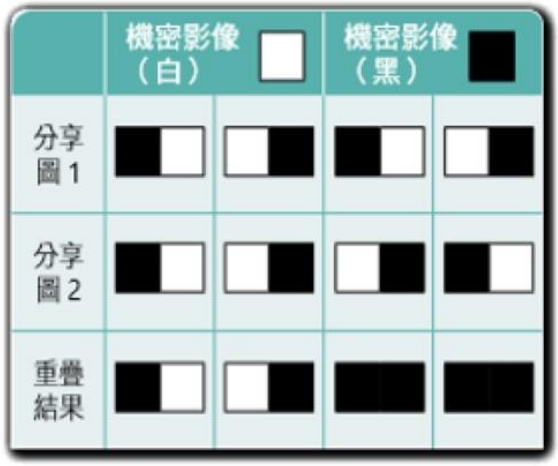

圖 3　1 × 2 視覺安全

視覺安全原理在於人類的視覺系統在辨識影像時，是根據一像素與周圍像素所產生的對比效果。而人類視覺系統無法清

楚的辨識出每一個像素值，只能感覺得出來一塊區域所呈現的效果，所以在此方法中，黑色以全黑來表示，而白色以一黑一白來表示。整體看起來，它就和黑色產生對比，因此人類的視覺系統就會將一黑一白認定為白色。接著來聊聊視覺密碼之有趣應用。

一張圖勝萬言書

是否你已看出端倪了呢？從圖 4 各種視覺辨識安全設定畫面中可以看到不再是輸入記憶中的資料，而是眼睛要開始說話了，要開「眼／演」了。先看看你是不是人類？若你說是，那麼繼續問你，你看到什麼，看到卡車嗎？看到飛機嗎？這可不能胡亂比畫勾選的，一旦眼睛看錯了，錯把機車看成卡車，誤把輪船看成飛機，胡亂瞎猜，系統可不隨便買單，直接“reject”地「翻你白眼」把你擋在門外，要你再來一次。幾次後再亂玩，可是會被停權而「拒絕再玩」的。視力測驗不再只是眼科醫生的專利，視覺安全在我們資安科技裡竟也開始軋上一腳，還是重要關鍵呢。

再以我們的好朋友孫悟空與牛魔王這搭檔唱雙簧來做些概念說明視覺安全的玩味與驚奇。老孫與老牛這兩位好友，事先都先分享彼此的「Shares」，也就是老孫有自己的黑白亂碼「Share 1」，也有老牛的黑白亂碼「Share 2」；相對地，老牛有自己的黑白亂碼「Share 2」，也有老孫的黑白亂碼「Share 1」。若老孫欲與老牛設定「碰面時間」為「Nov. 16, 2021」，即用內含「Nov. 16, 2021」的影像內容，並依據老牛的 Share 2 產生 Share 1′，再送

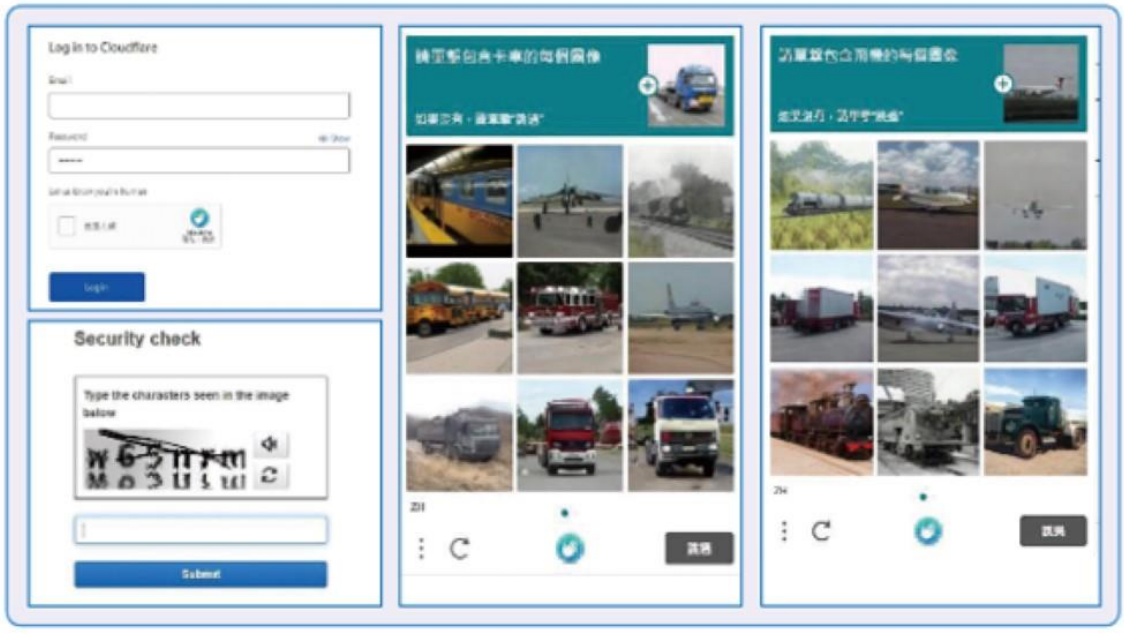

圖 4　視覺辨識安全設定

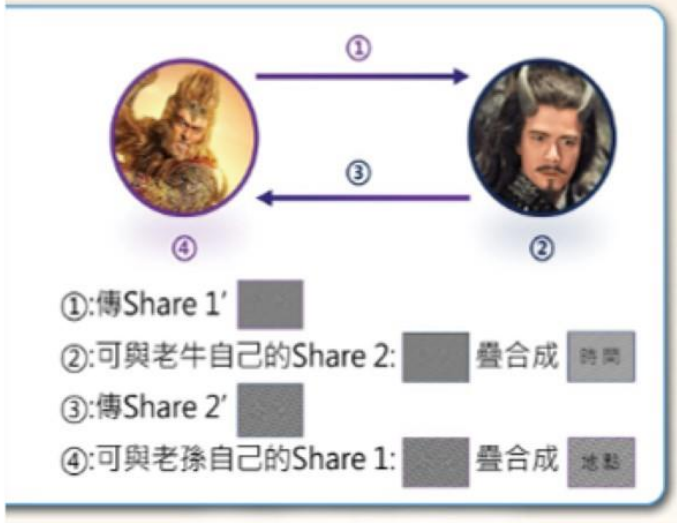

圖5　視覺安全的運作模式

給老牛。老牛收到後用自己的 Share 2 與 Share 1' 疊和後，眼睛會看見影像內容為「Nov. 16, 2021」，得以分享祕密訊息。相對地，老牛傳「神祕地點」給老孫也是一樣的概念。過程裡別人只能霧煞煞的看到傳送亂碼的 Share 1' 或 Share 2'，而且每次的時間與地點內容不同，所傳送的 Share 1' 或 Share 2' 也會跟著變變變。

眼睛除了「放電」，也會「計算」

Charming Eyes 一旦融入我們的資安生活，文學殿堂的靈魂之窗也得昇華為科技資安神守護，多了項頭銜讓我們放心享受資安生活。這是豐富有趣、耐人尋味、各種驚訝形容詞下的多媒體資訊時代。你應該從沒想過原來我們的 Eyes 除了「放電」也會「計算」，在眨眼間即「計算」（解密）出正確的訊息，看到什麼、寫出什麼、判讀出什麼，輸入系統裡，瞬間 decode it。

資安生活時代，我們透過電腦、手機節省了許多繁瑣的工作程序，想當然，電腦、手機也儲存了個資、帳號、密碼、各式生活理財的重要資訊在其中，這些都是為了減輕我們記憶負擔。科技成為我們最重視的好朋友，「不離不棄」，24 小時守著手機、等著「他」／「她」，堪稱情人等級的待遇。然而，好友一旦變臉，遭到入侵，帳號密碼盜用下，瞬間所有祕密將全部曝光。是否也喚起我們內心最深層的思維，還是天然的最好，我們與生俱來自然而迷人的 Eyes 是最好的朋友，永遠貼身伴隨著你，永遠不會被「盜用」（入侵），也是最值得信賴的守護神。

視覺安全在資訊科技裡可真是讓我們看到科技再發達，終究還是回到我們人類身上的眼「神守護」，才是「資安」的「自」在與「資安」的「安」心，原來資安裡已有著科技蘊涵「人」、「機」、「心」相互融入合一的精髓了。

社團法人台灣 E 化資安分析管理協會（ESAM）

中央警察大學資訊密碼暨建構實驗室（ICCL）