



公務機密

資訊安全維護



我朋友參加比賽，麻煩幫忙投個票謝謝，<http://www.lamaswinder.com.tw>，FB登入就可以了。



同學~那是什麼樣的比賽啊？為什麼要FB登入呢？

不亂開可疑的網站

不知名網站不要隨便連結瀏覽，如果有人叫你連結網站、投票、衝人氣等等，請先確認該訊息是否為本人所發出，是否為惡意網址，知不知道啊？

資安時事案例

小心駭客就在身邊

存款恐遭竊！亂掃QR Code「密碼被看光」學4招自保

個人資料保護法

掌握個人資料安全守則！減少詐騙騷擾

生活中的資安

鑑識&資安

數位學習

110年彰雲嘉數位機會中心資安小講座-我的密碼不好猜



資料來源：／  網軟 InterSoft 股份有限公司

要認識駭客常見手法就一定要先介紹到社交工程，駭客主要會利用社交工程的伎倆來欺騙您的個資，像是登入的帳號資訊更厲害一點還會騙走你網銀的資料，一不小心苦賺來的血汗錢全都不見，到時就真的欲哭無淚拉！

常見的攻擊方式：

利用電話佯裝資訊人員，騙取帳號及通行碼。

偽裝委外廠商之維護人員或上級單位人員，騙取帳號及通行碼。

利用電子郵件誘騙使用者登入偽裝之網站以騙取帳號及通行碼，如網路釣魚。(駭客常見攻擊手法)

利用電子郵件誘騙使用者開啟檔案、圖片，以植入惡意程式、暗中收集機敏性資料。

利用提供工具、檔案、圖片為幌子，誘騙使用者下載，如偽裝的修補程式、p2p 下載軟體、工具軟體等，乘機植入惡意程式、暗中收集機敏性資料。

利用即時通訊軟體如 MSN，偽裝親友來訊，誘騙點選來訊中之連結後中毒。

社交工程雖然利用人性弱點來騙取機敏資料，讓人覺得防不勝防，但只要隨時提高警覺，注意以下防駭 1 2 3 即可避免駭客攻擊造成傷害。

1 步建立資訊安全觀念：

- 隨時留意資安新聞與公告

2 招提升設備安全：

- 作業系統持續更新到最新版本
- 安裝防毒軟體，啟用即時防護，每週定期掃毒

3 不預防網路釣魚：

- 不開啟來源不明郵件：發現可疑信件不要開啟
- 不輕易下載附檔：不輕易打開、下載郵件中的附件檔
- 不隨意點及連結：不隨意點擊郵件中夾帶的網址連結



存款恐遭竊！

亂掃QR Code「密碼被看光」學4招自保



TVBS新聞 編輯 蔡明亘 報導 發佈時間：2022/01/20

新冠肺炎疫情影響加上電子支付越來越普及，民眾生活中經常需要拿出手機掃描QR code實聯制或付款，已經成為日常生活的一部分，不過如今卻要小心網路犯罪份子「竊改連結」，使用者導向的網站恐變成會竊取用戶個資與帳戶資訊的惡意平台。

美國聯邦調查局（FBI）近日發布公告指出，QR code提供快速連結網站、下載應用程式或線上付款等功能，尤其在疫情時代，使用QR code的人越來越多，如今卻有駭客利用這項技術，竊改連結使不知情的人被導向惡意網站，甚至還可能嵌入惡意軟體，誘導用戶輸入帳號密碼，進而獲得行動裝置的位置訊息和財務資訊，使用者帳戶裡的錢財就有危險了。

其中提到一項新興手法，就是透過貼紙覆蓋住店家原本的QR code，讓民眾在毫無防備的情況下，將個人資訊傳給駭客。FBI也說，雖然QR code技術本身是無害的，但民眾在透過QR code連結輸入財務資訊時，務必要謹慎，相關單位不保證能追回被轉走的資金。

至於民眾該如何自保？FBI建議4點，每次掃描QR code時，都要留意網址是否有拼音可疑之處，或正在掃描的QR code有沒有被貼紙覆蓋住，且不要透過QR code下載APP應用程式，盡量從App Store或Google Play商店等官方平台進行安裝，最後則是要與可信任的網站、電話或相關管道聯繫查證，別完全相信QR code顯示出的資訊。

《TVBS》提醒您：

因應新冠肺炎疫情，疾管署持續疫情監測與邊境管制措施，如有疑似症狀，請撥打：1922專線，或 0800-001922。

保護隱私 安全無慮

掌握個人資料安全守則！減少詐騙騷擾

資料來源：經濟部商業司

犯罪集團透過資料拼圖的手法，從A網站得知民眾的基本個資，從B網站得知近日消費內容，兩相組合，就可以編造天衣無縫的釣魚郵件，或精巧的詐騙話術，盡量不要讓個資被完整蒐集，就能減少被詐騙成功的機會。

公務機密維護宣導標語

依公務員服務法第4條：

公務員有絕對保守政府

機關機密之義務，無論

是否主管事務，均不得

洩漏，退職亦同。





鑑識 & 資安 buddy buddy

資料來源:清流雙月刊 33

◆社團法人台灣 E 化資安分析管理協會理事長、中央警察大學資訊密碼暨建構實驗室 (ICCL) — 王旭正教授

鑑識—判斷真假的代名詞

鑑識這字眼，直接聯想，就是追查新聞事件裡犯罪的軌跡。在臺灣擁有槍枝，甚至使用槍枝犯罪，那可是不得了的事件啊！從推敲的瞬間開始，就需要「鑑識」，因為由現場所遺留的子彈，可以推測槍枝種類，並進一步獲得彈道落點曲線等數據，抽絲剝繭地還原現場。是呀，這就是「鑑識」給人的印象—專業、判斷真假、還原事實。

訊息傳遞，「鑑識」需派上用場

然在這資訊時代裡，鑑識再也不單純只是專業形象而已，在人手一機，所有訊息都通聯的情況下，不經意間就會有各式的互動。訊息的傳遞怎會跟「鑑識」有關係呢？這可是有趣的事呢。還記得我們在前二期提到的網路嗎？現在的資訊網路無遠弗屆，人們也是人手一機，隨時隨地在滑手機。透過手機，隨時上網找資料，應付工作需求或作為報告參考依據；也經



網路釣魚利用盲點設陷，在人眼對文字、圖像辨識的模糊下，讓人被導入惡意程式、病毒而成為受害者。

常在手機操作網路下單、交易買賣，手機網路的便利，使我們不經意成為訊息、資料的傳送者，亦或是接收者。當身為傳送者（主動角色），即是將所知道、擁有、經手的訊息，主動經由網路，在各個時間（anytime）傳遞到各個可到達的人（anyone）與地方（anywhere）。

主動者還有可能誤觸網路裡設下的圈套陷阱，您經常聽到的「網路釣魚」就是如此。設陷者用各式盲點，針對人眼對文字、圖像辨識模糊與好奇，例如“ICCL”與“iccl”，您有無看到前者的“I”是後者的“l”呢？讓您不經意進入異想新鮮的世界，自以為「樂透了」、「中獎了」而喜不自勝，事實上，卻是逐步陷入迷網，被反導入非法惡意程式、病毒，進入主動者的手機（或工作、作業的電腦平臺）反遭監控、破壞與洩漏主動者的個資資訊。這種情況便落入俗話俚語所說的「公親變事主」，

無端惹出麻煩來了呢。而當主動者反倒成了被攻擊的受害者時，「鑑識」隨即派上用場，在資訊流、資料流、時間流、啥「關連流」裡，能逐次釐清因果關係，尋出真假異同，那即是鑑識觀念在主動端的重要並立見真章。

在這個互動頻繁的網路世界裡，主動者當然也會變身為被動的接收者角色。在被動者方面，一般會接收到3種型態的訊息，一則是文字訊息，二則是多媒體性訊息，三則是程式碼訊息。就網路資訊傳播發展早期，這3種型態裡，最令人畏懼的是第三種「程式碼」訊息，避之唯恐不及呀。

病毒程式發明者

程式碼訊息型態病毒來源可回溯自1960年代，由美國電話電報公司（AT&T）貝爾實驗室裡的幾個年輕小伙子所設計出來。原先動機只是好玩，設計出會覆蓋或破壞對方玩家電腦記憶體的程式，由於病毒（遊戲）程式的原始碼很小，使得此程式極容易被複製，而具有高存活率，也會攻擊與破壞另外的病毒（遊戲）程式，這就是程式設計者與玩家認定的最有趣之處——在相互攻防裡，取得最終的勝利，呵呵，換言之，就是把對方程式（遊戲）完全消滅，讓「病毒」成功入侵系統。

1986年，巴基斯坦人製造出Brain病毒程式，讓全世界注意到病毒程式會影響到電腦的正常運作。臺灣在1999年也不遑

多讓，有一聞名世界的 CIH 病毒，即由臺灣年輕人所設計，讓當時亞洲災情極為慘烈。

這些程式碼訊息隨著時空科技的演進快速翻倍進展，早已集結各家「精華」、各路「險招」、行極「冰寒」於一身。從古早的遊戲病毒 (virus) 源起，進化成木馬程式 (Trojan Horse)，網蟲 (worm)、攻擊程式 (attack programming)，讓資安世代網民經常誤陷泥沼。

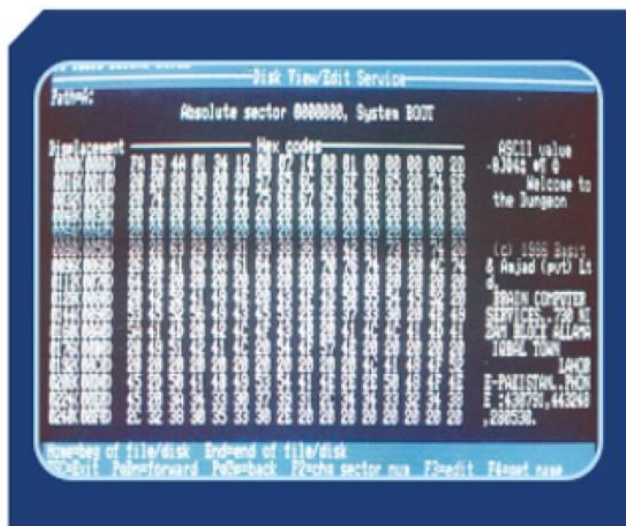
看不見的敵人最可怕

程式碼訊息雖最令人懼怕，卻也因敵在「明」，我們可藉「跡證」來辨識訊息「真假」，以避免踩到地雷。最直觀的方式，就是當收到不明的檔案或程式碼，尤其是具有執行能力的程式碼（例如副檔名

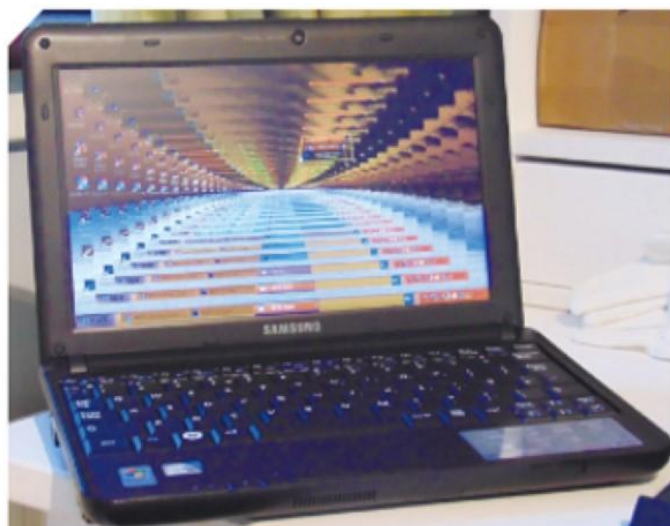
為 exe 者）時，即刻快閃刪除，就免惹到「無妄之災」。

再則，我們來到被動者接受訊息的第二種型態，那就是多媒體訊息。多媒體訊息在資安領域裡，是有別於密碼學 (cryptography) 的，我們稱為偽裝學 (steganography)，兩者最大不同在於「偽裝」二字，即「有看沒有懂」，亦即英文「Seeing the unseen」。以大自然生態為例，許多動植物都是偽裝專家，就像變色龍般，能隱藏於樹叢枯枝中，然後隨著綠葉枯樹的色澤而進行調變其身體顏色，讓食物鏈上層的獵食者，瞬間看不見其蹤跡，其實牠非「消失無蹤」而是「近在眼前」呢！

偽裝，不只發生在大自然裡，在生存遊戲中，更是「適者生存」的重要工具。



1986年，巴基斯坦人製造出 Brain 病毒程式，此病毒會感染開機磁區，影響電腦正常運作。(Photo Credit: Avinash Meeto, <https://commons.wikimedia.org/wiki/File:Brain-virus.jpg>)



「木馬」是一種後門程式，駭客用其盜取使用者的個人訊息，甚至進行遠端控制。(Photo Credit: BrayLockBoy, https://commons.wikimedia.org/wiki/File:MEMZ_Trojan_running_on_Samsung_N130_13_December_2019.jpg)

人類歷史在偽裝運用上頗精彩絕倫，尤其在戰爭史實上，最讓人嘖嘖稱奇。看似無奇的一頭秀髮，當剃光頭髮後，竟看到機密訊息，得以完成戰事攻防裡，祕密通訊的目的。

霧裡看花，花還是花？

在當代，我們所接觸到的訊息更具變化，真真假假、五花八門。為何包裝程式碼的多媒體訊息能如此活躍？主要是因人類眼睛對於色彩具有失真的容忍度，也就是我們玩笑話裡的「朦朧美」、「霧裡看花、花還是花」的感官意識。

對於影像，當人腦認定有何涵義時，是草、是河、是山、是屋，那是深刻烙印在腦海，不會因模糊而改變的印象。而數位時代，構成數位影像圖的每個像素，若改變裡頭一些像素資料時，且在視覺容忍度與感官意識可接受下，人眼將無法識別其差異性，此時多媒體影像所包裹的訊息就可以混水摸魚，逃過一劫，達到得以祕密傳遞的目的。

當然，對於訊息暫時接觸者所接觸到的是一張、一份多媒體假訊息的影像圖，所認定也是一份貨真價實的、具有意義的多媒體資訊，所以暫時接觸者因此以為是「真訊息」。然對為達成訊息傳遞的通訊雙方一即訊息的傳送者與接受者，目的是要讓中間的暫時接觸者，看到「假訊息」，即誤以為影像圖是「真訊息」。到此，真假之間，是



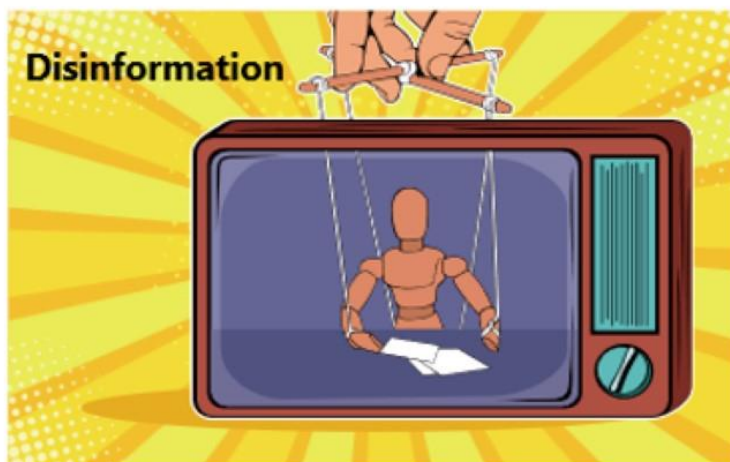
大自然生態中，許多動植物都是偽裝專家，多媒體訊息在資安領域裡亦為偽裝大師。

否您也看得霧裡看花，不再是花，而是「霧煞煞」了。

偽裝之意，在於欺敵，在第二種的多媒體訊息形態裡，或許無誤導於呈現多媒體訊息時的具體內容（有論無意或蓄意），因該訊息意在偽裝多媒體內涵裡的真實祕密。

Misinformation 與 Disinformation

然而被動者的訊息接收裡，第一種訊息型態的文字訊息，是最令人毫無防備的。若其為假訊息，將是這3種訊息型態中影響最為深遠的訊息。對於假訊息，歐洲理事會有一相關名稱為「資訊失序」／「Disinformation」（原文：Information that is false and deliberately created to harm a person, social group, organization or country），其是指經過刻意編造，用以傷害個人、社會團體、組織或國家之訊息，目的在煽惑或鼓動人



Disinformation 是指經過刻意編造的錯誤訊息，用以傷害他人、組織或國家之訊息；Misinformation 為內容有虛假嫌疑，惟因缺乏惡意欺騙之意圖，故多屬誤傳。

心，藉以謀取某種政治或商業利益；另外「資訊失序」還有一種描述用語為「Misinformation」（原文：Information that is false, but not created with the intention of causing harm）則是指內容錯誤但目的並非為造成傷害而刻意創建的訊息。在假訊息之要件上，國際組織主張應符合真實性（fidelity）與目的性（intention），所以「Misinformation」雖內容有虛假嫌疑，惟因缺乏惡意欺騙之意圖，多屬誤傳性質之訊息。而「Disinformation」是目前較符合國際對假訊息之定義或共識，是有系統性的作假，企圖製造損害、影響特定人士或組織，導致社會紊亂，屬政府部門應該積極防處之範疇。

透過資安密碼技術 管理訊息傳送

對於文字的假訊息，咱資安科技裡的密碼技術，並不因此坐視不管，反倒有好的因應呢。回顧上一期的 PK（public key），在公開金鑰系統裡的使用，如果訊息的傳遞，由真實來源的傳送者在傳送的

過程中，加上與訊息緊密相關的驗證碼，那麼不就可以清楚地知道訊息是真、是假，有無被竄改。

在現代密碼技術中，有個重要名詞叫「HASH」，「HASH」這武器是能夠不管訊息有「山這麼高、海這麼深」，都可以變成一個短短的資料量，好像是神奇的魔術一樣。例如一個超大硬碟容量，可以變成一串短短字串，只要硬碟裡的一絲點位元或一根寒毛被動到，這短短字串就會變得不一樣。因此，當訊息在 HASH 第一次運算和 HASH 第二次運算後，結果都一樣，就代表這個硬碟裡的東西沒被動過，很神奇吧！

在假訊息訊傳遞充斥的世代裡，我們運用資安科技裡的密碼技術處理假訊息，就不用流於口水戰。有了這兩大法寶——「PK」還有「HASH」，假訊息就無所遁形了。發布訊息時使用 PK 系統，然後再進行比對，如果兩邊內容一樣，就可證明訊息是由真實來源端所提供。

處理機制裡，我們可先用 HASH 做訊息的處理，因為一般訊息較長，用 HASH 的技巧可變成比較短的訊息，而且用 HASH 也可以用來保證一旦訊息被更改後，可以很快地發現被竄改。因為一旦原始訊息的一個文字或一丁點的位元資料被改變，整個 HASH 的結果都會不一樣，接下來就是再用 PK 系統來產生驗證碼。以前兩期孫悟空與牛魔王的故事裡，我們稍作小技巧，增加了 HASH 技術，可立見真章，讓人一點就通。

這裡我們討論真、假訊息的兩種狀況，第一種訊息傳遞是無論訊息真假，但發布訊息的人是假（不對）的，舉例來講：今天要發布獎懲訊息，這種訊息不是每個人都

可以發布的，一定要是權責單位發布的。假設今天是路人甲、乙、丙說的，擅自發布的訊息都要打個問號，因為這些人不是權責單位。當然若是權責單位承辦人、發言人講的，那訊息可信度即是相對提高的。在 PK 系統的驗證碼比對中，真正權責單位的 PK 再搭配 HASH 的處理，能讓事實立即擺在眼前。

另外訊息傳遞的第二個情形是，權責單位的確發布事實訊息，但發布的訊息被蓄意先下架，內容遭竄改後，例如把褒獎令的內容改掉，再進行發布。此情形裡，發布的權責單位是對的，但是內容是被改過的。但是在這一個過程中加上一個 HASH，就可以把這問題爭議處降到最低，因為依照所提



圖 1 PK 系統與 HASH 的搭配處理



訊息漫飛時代，各式傳聞不斷，虛虛實實、假假真真，民眾看多假訊息之後，可能連政府發布的真訊息也不再相信了。

到的密碼技術概念，HASH 這武器可清楚證明訊息是否被造假竄改。例如，若今天褒獎令的訊息裡有相關人物數量的名額是「10」位，被修改成「9」位，就會發現所傳遞褒獎令的訊息經第二次 HASH 的運算後會很不一樣，所以搭配 PK 的 HASH 也是解決假訊息的關鍵技巧之一。

假做真時真亦假 假訊息竟成「網紅」？

訊息漫飛時代，各式傳聞不斷，虛虛實實、假假真真，套句紅樓夢賈寶玉的名言「假作真時真亦假」，因此當民眾看多假訊息之後，可能連政府發布的真訊息也不再相信了。

在資安科技裡，除了最為直觀認知的重要「隱私」保護外，另一訴求就是「鑑定」，也就是對於來源能清楚、對於訊息的真假判斷能有依據，得具有說服力。而「鑑識」即是在「鑑定」的各式場合、各式情境裡，在人為、人治世界的生活互動裡，無論有意、無意的侵犯裡，在所遺留的證據痕跡中，能抽絲剝繭、步步推理，找到真相、重建現場。資訊生活裡，我們使用的 3C 平臺讓我們更方便操作訊息，是傳遞訊息的主動者，也是接收訊息的被動者。在享受訊息多元化、知識普及化的同時，另一類資安危機也浮上檯面。真、假訊息在這些年來，成了「網紅」，不知覺淪為各式可能不當企圖運用的操作，得以混淆人的意識與判斷，影響生活，甚而造成社會問題與資安危機，甚至被科技犯罪利用得以獲利。現在藉由資安的密碼技術發揮，在人手一機的訊息來回裡，訊息得以「鑑識真假」。傳統的人腦思維判斷方式已轉化成資安科技的「鑑識」加乘確認，藉此得以保障「真假」訊息傳遞的真實性，減輕可能的權益損害，「鑑識」儼然成為資安生活中共生共存的 buddy buddy 新重要搭檔。



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)