

# 秘密 已經不再是 秘密？

◆ 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

科技越發達，隱私越具價值。現代資安科技重視「個人隱私」、「家庭隱私」、「國家隱私」、「國際隱私」，恰對照古云「修身」、「齊家」、「治國」、「平天下」，也自然畫點出「資安就是國安」的精髓。

## Security 和 Forensics 是搭檔 成為「SecForensics」趨勢

傳統鑑識 (Forensics) 不需與數位或電腦系統直接聯想，也不常發生，例如槍枝走火的判定、火災的火源在哪裡；然而，如今在數位洪流裡，卻在身邊、在把玩手机時，不知不覺就會有鑑識問題跑出來。

諸如大家的生活好朋友 LINE、FB 遭盜用，莫名地成為入侵攻擊事件的主角；民眾也會習慣性地藉 google 網路，期能獲得科技法律的諮詢與了解，進而尋求保障個人資料的安全等。所以 Security 和 Forensics 現今已是搭檔，經常綁在一起，兩者合體即為「SecForensics」，這詞是趨勢，也是資安生活時勢裡最重要核心觀念



在 LINE 裡，雖然大部分是好朋友，但在好友列表裡面也有可能是<sup>不</sup>經意加入的 LINE 好友。例如加商家為好友才能下載免費貼圖，逛街買東西要加店家的 LINE 才有打折等等。商家總會提供一些好處、優惠的方案給你。但在 10 個好處裡面，總有那麼一、兩個是準備要在你的手機裡面植入木馬。「最便宜的最貴！」就是抓住人們貪小便宜的心態，才會無時無刻有駭客入侵事件發生。

這些商家，偶爾會送些訊息到你的手機，可能會再提供一些網址請你按連結，不知不覺中，你的手機就會被植入木馬，不經意地被入侵了。這時就需要「數位鑑識」來解救了。



手機可以是一個資料庫、通訊器，但同時亦可能成為秘密暴露的出口。

## 驚人的現世報— 秘密已經不再是秘密

反過來，有時候我們也可能流程操作錯誤，而「不小心」入侵了別人的手機、電腦，雖非是故意的，但行為上就是已經被對方覺得你是在干擾他、入侵他了。無心之間擾亂了別人的系統，對方卻覺得就是你在作怪，入侵對方系統，無緣無故就被對方告了！「數位鑑識」裡證據會說話，可還你清白，卻也顯露了驚人的現世報—「秘密已經不再是秘密」。

為何「秘密已經不再是秘密」？手機可以是一個資料庫、資訊的來源，另一方面也是貼心的工具，能幫你存有許多不欲人知的秘密。而且如果真能成功地將木馬植入別人手機裡，就可以完全知道別人手機裡的狀況。手機還可以透過一些 APP 小程序去定位別人。這些軟體看似好用，可以直接呼朋引伴，也能清楚知道你在哪裡。啊，如此一來，秘密就已經不再是秘密了呀。

## 軟體「鑑識」與硬體「證據」 相輔相成

數位鑑識乃是使用科學技術進行搜集、鑑定、找出關聯性、運用各種技術將數位證據文件化，並找出與案件所需且相關的數位證據。數位證據有如電腦結構中之硬體，這些硬體散落在犯罪現場，需要

靠鑑識人員細心的將所有的證據一一找出，電腦若僅有硬體而沒有軟體的輔助，電腦硬體就像是英雄無用武之地，也由於電腦硬體與軟體的天作之合，才得以開啟電腦世代的新紀元。

反觀「鑑識」與「證據」的組合，互依互存有如天作之合的軟體「鑑識」與硬體「證據」，少了其中一種就無法發揮其作用。因此如果沒有「證據」的殘屑佇留，何來「鑑識」之推敲、溯衍，另一方面，沒有「鑑識」的抽絲剝繭，碎屑依然散落，就算有再多的證據也無「證明力」來證明犯罪事實。

### 如何從眾多證據中， 找到證明犯罪事實

了解數位鑑識與證據之關係後，最重要的是如何從眾多的證據中找到足以證明犯罪的事實；另一方面是利用數位鑑識工具及方法所萃取出來的證據，好好保存以免失去其證明犯罪之證據力及證明力。其中證據力，是一個水平的概念；證明力，則是垂直的概念。掌握愈多證據，愈多元化，就有愈強的證據力。而什麼是垂直的證明力？你可以從一根頭髮，判斷他是男生或女生（第一層）、年齡層（第二層），或是分析出這個人有哪些疾病（第三層），掌握愈多層次，代表證據證明力愈強！



「鑑識」就是將犯罪現場、證據及受害者與嫌疑人之間的關係與來龍去脈描述清楚。

「鑑識」是將事情弄得清清楚楚，是一個流程、一個說法，而整個過程當中，要有一些東西是實質、眼睛看得到的，就是所謂的「證據」。所以，要構成犯罪，需要具備的四個元素，第一個：真實的犯罪現場（網路上的虛擬、想像的，沒有留下痕跡的，是不成立；當有留下痕跡、紀錄、文字等，即可為成為證據的基本依據）；第二個：受害者；第三個：嫌疑人；第四個：證據。我們將整個過程、這四個元素的來龍去脈、兩兩的互動關係上，描述得非常清楚，這樣的一套過程模式，就是「鑑識」。

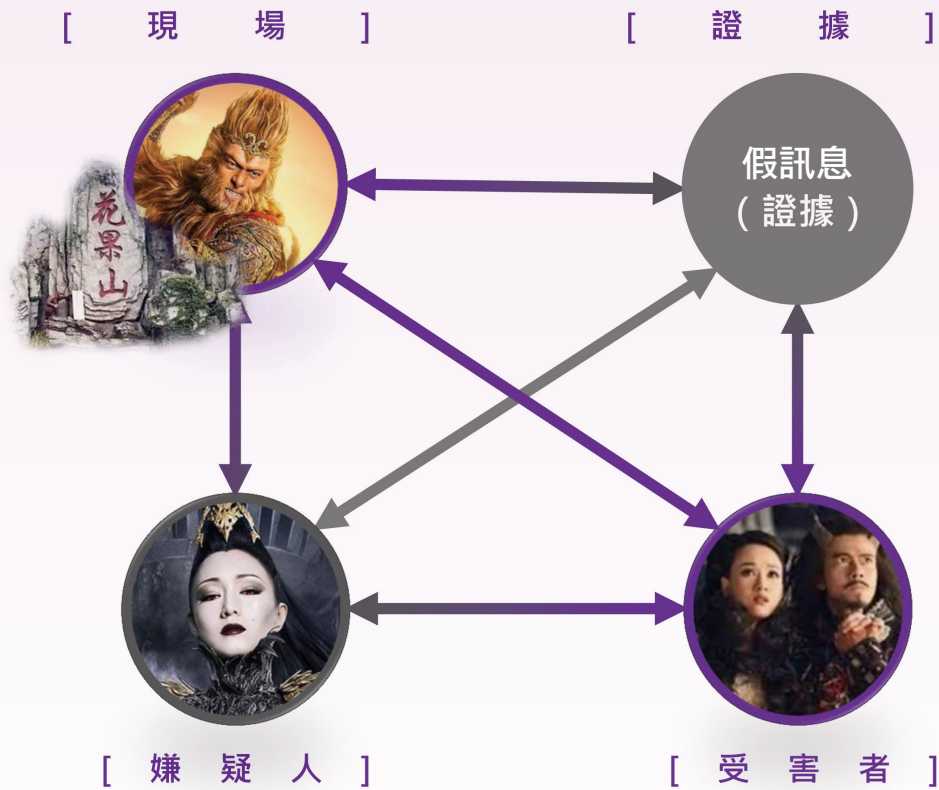


圖 1 數位鑑識的  $K_4$  系統面相

所以當手機犯罪，就需要將手機扣押，撈出各種可能的證據，再去定位一下犯罪現場在哪裡？誰是受害者？誰是可能的嫌疑人？到底做了什麼事的證據痕跡？證據和現場的關係？證據和受害者的關係？證據和嫌疑人的關係？還有嫌疑人和受害者的關係？受害者、嫌疑人為什麼會在現場？當把全部證據找得完完整整，整個犯罪過程弄得清清楚楚，才能真正地說服所有人。

圖 1 中，我們以數位鑑識的  $K_4$  完全圖說明如下，其中孫悟空的花果山為事件現場，白骨精為發布訊息的嫌疑人，發布的訊

息經資安的鑑識檢驗為假訊息證據，牛魔王與芭蕉公主為假訊息事件的受害者，此四元素的關係得呈現完全的相互關連性。

**由 RootKit 談「反鑑識」概念**

數位鑑識也有「反鑑識」的概念，RootKit（隱藏程式）就是比較趨向反鑑識（Anti-forensics）的概念，它不能讓別人知道它，但是它又嘗試在裡面扮演重要的角色。為什麼 RootKit 有點像反鑑識？「反鑑識主要是隱藏自己的身分不讓別人知道」。是啊，RootKit 是「隱藏程式」的概念，那 RootKit 的這種隱藏程式是為了做壞事？

還是在必要的時候讓自己發揮作用？其實 RootKit 以正面的角度來看，是系統管理者的重要助手，管理者是正面的機制，入侵者是負面、破壞者。

RootKit 本用於隱藏行程的功能，可對系統進行存取或將系統核心中所使用的行程隱藏起來，避免使用者在操作時不小心而影響到系統運作，出發點並非惡意。我們這個社會是一個正面的正義模式，當我們社會機制遭到破壞的時候，就可以透過這個正義模式的機制，讓破壞攻擊降到最低。但如果有人有心將這個正面的機制拿來破壞社會次序，那它還是會變成負面的。例如警察向來代表正義力量，但若他被人收買，變成負面的去做壞事，反而造成更

大的社會危機。引用這些譬喻是為了說明，當駭客利用此手法變向操作 RootKit 時，反會將木馬程式等隱藏到作業系統中，從而造成意料之外的危險，那麼 Rootkit 將被視為是非常危險的惡意軟體。

### 反鑑識的正向價值觀

數位鑑識與反鑑識，並不是狹隘的相反定位而是相互為用。反鑑識主要用意是保護商業利益，隱藏一些機密的資訊，反鑑識裡的證據不能被找到。然反鑑識不是「把犯罪的證據藏起來」，因為如果說「反鑑識是把犯罪的證據藏起來」，大帽子一扣，大家都會怕，聽了會心驚膽跳。例如一間商店寫「殺人放火店」，裡面賣凶器，

```
static int __init procfs_init(void)
{
    //new entry in proc root with 666 rights
    proc_rtkit = create_proc_entry("rtkit", 0666, NULL);
    if (proc_rtkit == NULL) return 0;
    proc_root = proc_rtkit->parent;
    if (proc_root == NULL || strcmp(proc_root->name, "/proc") != 0) {
        return 0;
    }
    proc_rtkit->read_proc = rtkit_read;
    proc_rtkit->write_proc = rtkit_write;

    //MODULE INIT/EXIT
    static int __init rootkit_init(void)
    {
        if (!procfs_init() || !fs_init()) {
            procfs_clean();
            fs_clean();
            return 1;
        }
        module_hide();

        return 0;
    }

    static void __exit rootkit_exit(void)
    {
        procfs_clean();
        fs_clean();
    }

    module_init(rootkit_init);
    module_exit(rootkit_exit);
}
```

RootKit 是系統管理者的重要助手，但若遭入侵者利用，就會變成危險的破壞者。（Photo Credit: Christiaan Colen, <https://www.flickr.com/photos/christiaancolen/21133308006>）

一定會倒，因為非社會正義當然立即會被取締關門。又若你貼文在 FB 上標明「殺人放火店」，按讚的人也都有可能被調查是否有犯罪動機。

現代巡邏有所謂的「網路巡邏」，在「科技—資安—鑑識」已是國際化的趨勢下，傳統巡邏也在資訊時代洪流裡演化成網路巡邏。就如剛才所說，若在 FB 上張貼具有擾亂社會秩序嫌疑內容時，也會很快被社會公權力單位之網路巡邏者發現，並迅速地被抑制。

藉此我們想說明「反鑑識」，並不是狹隘地將證據湮滅掉來鼓勵犯罪，而是在保護商業利益方面的智慧財產權（例如網站新聞內容是有財產權的），資訊隱藏、資料偽裝亦或是軍事間諜、線民臥底等，也有反鑑識的正面價值觀，能協助情報偵蒐，裡應外合地破案，透過迂迴方式以打擊危害社會秩序的各式非法行為，這也是「反鑑識」的最原始正面的價值觀。

## 運籌帷幄，決勝於網路之內

生活中一直都存在傳統犯罪，有了電腦犯罪之後，還是會有西瓜刀、棒球棍，總不能拿手機對砍吧！但科技犯罪遠比傳統犯罪誇張、無遠弗屆，戴著鴨舌帽搶銀行的行為已落伍，以「高科技方式搶銀行」正時興，如同「運籌帷幄，決勝於千里之外」，在看不到的地方算計才是勝敗關鍵。而網路犯罪產生的經濟災損，幾乎都是上億元起跳，超乎想像，也不是以棒球棍回擊就可了結的。

祕密或證據從「天知、地知、你知、我知」之時空背景，在數位鑑識時代裡成了「錯、錯、錯、錯」之大家都知道的祕密，「祕密已經不再是祕密」；證據全留存在系統、手機、電腦、網路，近在我們身邊！資安科技與個資已是密不可分的重要貼身好朋友，而懂資安、找證據（鑑識）、保障個資祕密（反鑑識）成為在現代生活中保護自己的必備武器，藉此，也才能自在地享受科技帶來的便利。



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)



# 淺談 資通安全 最弱環節

◆ 臺北中正高中資訊組長 — 李詩婷

資通安全的整體安全強度，取決於系統中最弱環節，而政府機關及企業組織中，「人」往往是最容易造成資安事件的原因。





## 最弱環節 最易被入侵

在「不可能的任務」電影中，阿湯哥飾演的伊森韓特（Ethan Hunt）往往會因任務需求，不得不祕密入侵高度防備的企業組織或政府機關，而作為一個正派特務，絕不會拿猛烈火力來硬碰硬，因此，小組人員就會開始進行行前戰略會議，包含研究分析建築物架構、門禁及警衛編制、內部員工組織分布等所有可能的入侵管道，以從中找出一絲一毫的入侵機會。這種原理不難明白，即是分析對方最容易侵入之弱點，以提高成功的機會。

在「不可能的任務」電影中，阿湯哥飾演的伊森韓特（Ethan Hunt），出任務前會分析目標地點之建築結構、門禁及警衛編制，以從中找出最容易侵入之弱點。這種原理不難明白，即是分析對方弱點，以提高成功侵入的機會。對比資安防護，亦取決於系統中的最弱環節，而「人」就是最易侵入的關鍵點。（Photo Credit: Paramount Pictures）

全的整體安全強度，取決於系統中最弱環節（Weakest Link）」，而「人」就是被公認為是這裡所指的最弱環節，從日益猖獗的網絡釣魚詐騙似乎也印證了此一論點，不管是臉書、LINE，或是簡訊，總是有推陳出新的新詐騙內容。

## 「人」是資安的最弱環節

近年重大資安事件層出不窮，政府機關及企業組織無不聞駭色變，紛紛提高了資安防護的經費與人力以對抗駭客入侵。但在資通安全領域有一句名言，「資通安

## 假冒銀行發送簡訊 客戶損失數百萬元

以近期的新聞事件為例，110年1月底，駭客偽冒國泰世華網銀發送釣魚簡訊，

## 提醒您若收到假冒本行名義或來路不明之簡訊訊息，切勿相信或點選連結，以維護您的權益

國泰世華提醒您：

本行不會主動請您登入網路銀行綁定用戶資料。

使用網頁版網路銀行，請務必再三檢查應為以下正確網址(<https://www.cathaybk.com.tw/>)，若您收到來路不明之簡訊訊息，假冒本行名義請您輸入代號密碼或個人資料，那是假的！切勿相信！如您近日已於可疑網址輸入網路銀行的用戶代號及網銀密碼，建議您儘速進行更改。如有任何疑問，請聯繫165反詐騙諮詢專線或進線本行客服專線：02-2383-1000 或 0800-818-001。

為保障App使用安全，本行將調整以下功能：

1. 交易認證碼申請（自民國110年3月19日起重新開放交易認證碼申請，申請成功後滿24小時始得於線上交易使用交易認證碼驗證）。
2. 非約定轉帳限額調整（自民國110年4月6日起本行非約定轉帳之預設交易限額調整為每筆新臺幣5萬元整，每日新臺幣10萬元整，每月新臺幣20萬元整，若您前已透過臨櫃或網銀App完成設定非約定轉帳之交易限額者，將維持您原設定之交易限額，若需要調整請親臨本行任一分行櫃檯辦理）。

造成您的不便，敬請見諒

國泰世華銀行已在官網及 APP 上宣導相關資訊，強調「銀行不會主動要求用戶登入網路銀行來綁定用戶資料」。（圖片來源：國泰世華官方網站 <https://www.cathaybk.com.tw/cathaybk/personal/news/announcement/2021/012801announceinfo>；<https://www.cathaybk.com.tw/cathaybk/campaign/ebanking/2021fraud>）



內容為：「您的銀行帳戶顯示異常，請立即登入綁定用戶資料，否則帳戶將凍結使用」，訊息下方同時附上銀行網址要求民眾登入網路銀行。許多人驚見此訊息，心急立即點進此連結網站，而不幸被竊取其用戶代號及密碼，已有多位國泰世華網銀用戶上當；帳戶內資金被盜轉出去，短短3天內就有21人被害，損失金額高達三百萬元。對此，國泰世華銀行已在官網及APP上宣導相關資訊並暫時關閉APP部分功能，並強調「銀行不會主動要求用戶登入網路銀行來綁定用戶資料」。

## 網路釣魚常見手法

通常駭客若要成功進行網路釣魚，首先必須精心偽裝連結網址，常用手法如將字母「i」改以數字「1」取代，或是字母「w」改以連續兩個「vv」取代等方式，而此次國泰世華詐騙案所使用的偽裝手法就是將真實網址「[www.cathaybk.com](http://www.cathaybk.com)」改為「[www.cathay-bk.com](http://www.cathay-bk.com)」，由於網址名稱太過接近，難怪用戶難以察覺，點了連結後當然就會被導向偽裝的惡意網站。

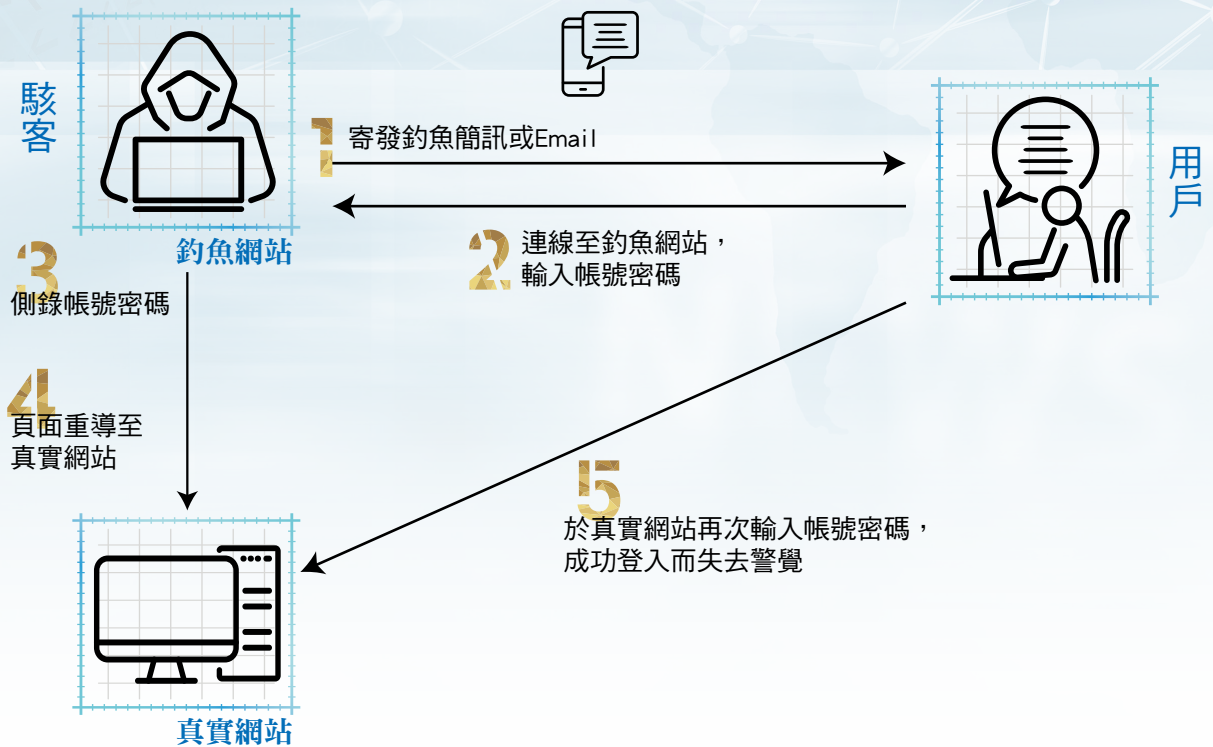


圖 1 釣魚網站非法獲取資料流程

駭客誘騙用戶點擊網址連結只是第一步，第二步則是要騙取用戶之帳號密碼，所以這時就必須利用事先架設的釣魚網站，且其網頁頁面必須跟真實網頁十分近似，包含標題、圖片及登入介面等皆需高度雷同，才能讓用戶放心點選。由於釣魚網站製作無法與真實網站完全相符，因此此時若用戶留心的話，會發現釣魚網站上的部分按鈕或連結功能可能無法點選或使用，或是輸入帳號密碼後卻沒有任何反應。更有甚者，為了不讓用戶察覺到此為釣魚網站，過往案例顯示，駭客可能在用戶輸入帳號密碼後，立即將頁面導向至真實網站的登入頁面，讓用戶誤以為是自己輸入錯誤所導致，而當用戶再次輸入帳號密碼

並成功登入真實網站後，就不會察覺到第一次所輸入的帳號密碼，其實早已被駭客盜錄下來。

### 防範網路釣魚之自救方式

若民眾收到任何要求登入網路銀行的通知，建議可先與銀行確認，切勿直接在簡訊上點擊連結。另為避免不小心點擊到來歷不明的網址，建議民眾可以養成記住常用銀行網址的習慣，或將銀行網址加入瀏覽器書籤，另外也可利用搜尋引擎找到正確網站，以減少被釣魚網站詐騙的風險。

一旦懷疑自己可能已經中招，除儘速確認帳戶狀態外，另外應該趕快變更密碼，

表 1 2021 農曆年前偽冒臺灣金融機關釣魚簡訊及網站情形

日期	內容	追查釣魚網站數目	受害情況
2021/1/6	<b>釣魚郵件、釣魚網站</b> 疑似偽冒中華郵政寄送郵件，竊取個資。	1 個	不確定
2021/1/27	<b>釣魚簡訊、釣魚網站</b> 【國泰世華】您的銀行帳戶顯示異常，請立即登入綁定用戶資料，否則帳戶將凍結使用。	6 個	據警方 2 月 6 日統計，已接獲 89 件通報，25 件被害人帳戶已遭盜用，損失金額高達 518 萬元。
2021/2/5	<b>釣魚簡訊、釣魚網站</b> 【台新銀行】您好，由於網路銀行版本更新，請於 2 月 6 日前登入進行驗證，否則將停用您的使用權限，超時請至臨櫃辦理。	17 個	據警方 2 月 6 日統計，已接獲 10 件通報，7 件被害人帳戶已遭盜用，損失金額高達 55 萬元。
2021/2/9	<b>釣魚網站</b> 疑似偽冒富邦人壽官方網站，竊取個資。	1 個	不確定
2021/2/9	<b>釣魚簡訊、釣魚網站</b> 【中國信託】你的網路銀行更新失敗，請立即輸入你的驗證碼以更新資料，超時請重新輸入。	11 個	據警方 2 月 9 日統計，已接獲 1 件通報，尚未有受害者報案。

資料來源：iThome，<https://www.ithome.com.tw/news/142711>。

以搶在駭客前保護好帳戶資金。另外，若自己曾在多個不同網路服務中使用同一組帳號密碼，例如網路銀行、個人信箱、社群媒體及購物網站等，也必須一併更換，以避免駭客利用所竊取到之帳密資料進行多方嘗試。

### 資安防護無假期 提高警覺最要緊

網路釣魚或網路詐騙，除了針對個人進行資金詐騙外，駭客在入侵機關及企業組織時，也常選擇從機關及企業組織資安防護的最弱環節下手—即人心，利用釣魚信件或簡訊等方式為攻擊發起點，對員工進行詐騙，如此可避免直接與防火牆等資安防護設備硬碰硬，提高攻擊效率。儘管

**這不是  
打錯我的名字挑戰  
而是釣魚網站**

catheydf.com catheydf.com  
catheydf.com cathaydk.com  
cathaydw.com catheydf.com  
ctahaybk.com ctahaybk.com

提醒您春節期間  
詐騙猖獗形式百百種

## #多看一眼 詐騙不走眼

提高警覺守護資訊安全  
[www.cathaybk.com.tw](http://www.cathaybk.com.tw)

為防止釣魚訊息持續橫行，各大銀行彼此串聯，共同於今年農曆春節前在各自的臉書上張貼有趣的防詐騙文案，提醒民眾詐騙集團全年無休，要隨時防範。（資料來源：國泰世華臉書粉絲專頁，<https://zh-tw.facebook.com/cathayunitedbank/photos/a.160335250820488/1811446399042690>）

目前市面上存在惡意網址檢測及惡意郵件過濾等資安產品防護功能，但駭客釣魚手法也在進化，因此，有效培養員工的警覺心、強化資安意識及定期教育訓練，才是守護資安之最佳對策。