智慧時代新生活
~資安新趨勢

講師　　呂守箴

大綱

- 近期網路釣魚探討：
  - 通訊軟體詐騙手法
  - 簡訊詐騙手法
  - 電子支付詐騙手法
- 帳號密碼的新風險：
  - 多因子認證 (MFA)
  - 無密碼身分識別 (FIDO)
  - 深偽技術 (Deepfake)
- 常見資安事件宣導：
  - 物聯網(IoT)與監視攝影機
  - 郵件社交工程
- 資安法規摘要：
  - 個人資料保護法(個資法)

- 講師： 呂守箴
- E-Mail：shooujen@gmail.com

- 講師資料：goo.gl/Uzv2BW (注意英文大小寫)

- 智慧時代新生活 YouTube 頻道：youtube.com/OpenBlueSmartLife
- 智慧時代新生活 FB 粉絲頁：facebook.com/SmartEraNewLife

- 個人 Facebook (FB)：facebook.com/openblue
- 個人 Instagram (IG)：instagram.com/openblue.ig
- 個人 YouTube 頻道：youtube.com/openblue

講師資料：
請掃描

教學影片：
youtube.com/OpenBlueSmartLife

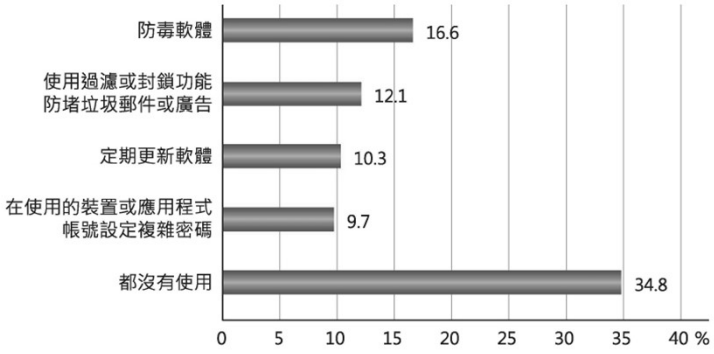
粉絲專頁：
facebook.com/SmartEraNewLife

▌逾3成民眾沒有使用任何措施保護上網安全

◆111 年度現況

我國 16 歲以上民眾為保護上網安全所採取之措施，以使用防毒軟體（16.6%）的比例最高，其次為使用過濾或封鎖功能防堵垃圾郵件或廣告（12.1%）、定期更新軟體（10.3%）、在使用的裝置或應用程式帳號（含信箱、社群媒體、第三方支付軟體等）設定複雜密碼（9.7%），但有超過 3 成（34.8%）的民眾沒有使用任何措施來保護上網安全。

採取哪些措施來保護上網安全（前五名）



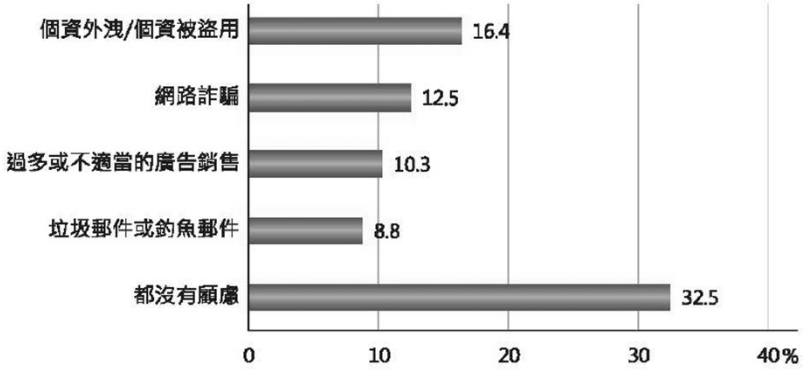
Base：N=1,129，複選（有使用網路者）

▌個資外洩與網路詐騙為網路使用顧慮之最

◆111 年度現況

我國 16 歲以上民眾對於使用網路的顧慮，以個資外洩 / 個資被盜用（16.4%）比例最高，其次分別為網路詐騙（12.5%）、過多或不適當的廣告銷售（10.3%）。另外，約有 32.5% 的民眾對於使用網路都沒有顧慮。

使用網路的顧慮（前五名）



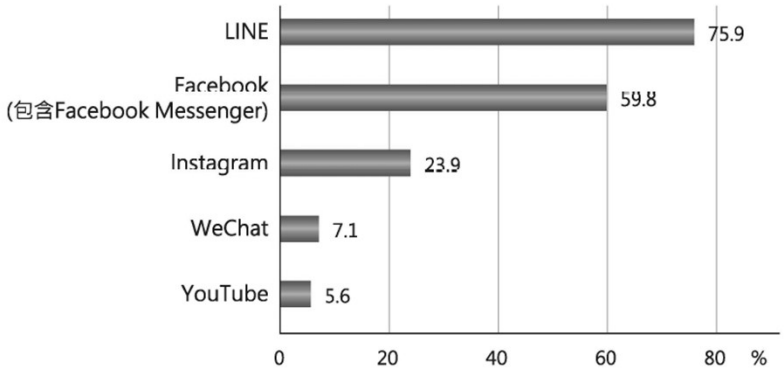
Base：N=1,309，複選

LINE使用率逾7成5，連年穩坐第一

◆111 年度現況

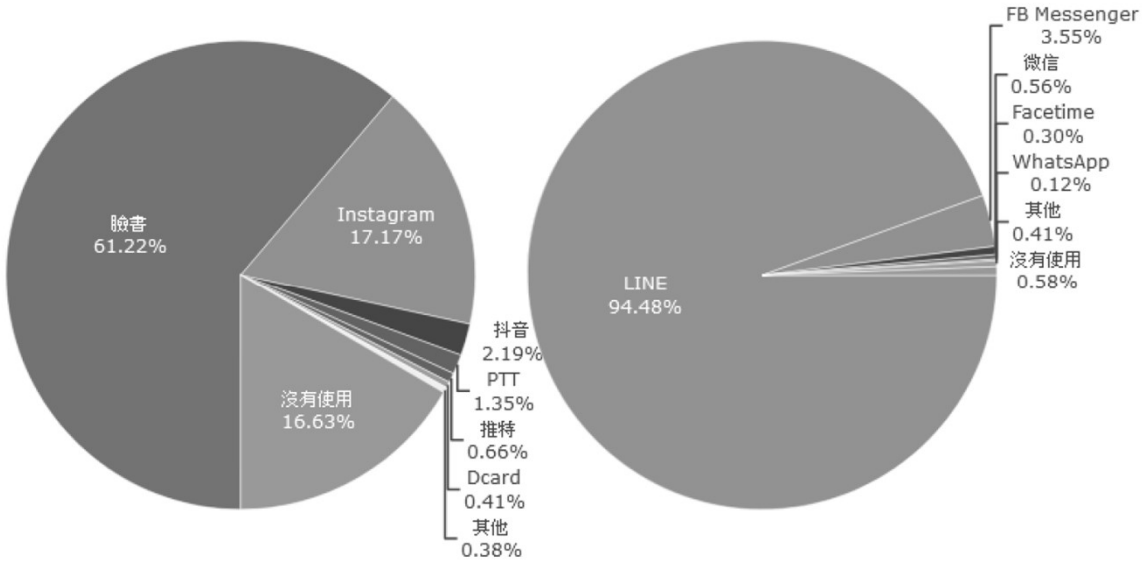
我國民眾擁有仍在使用的社群媒體或即時通訊帳號，以 LINE 的比例最高，達 75.9%，其次為 Facebook（包含 Facebook Messenger）（59.8%）、Instagram（23.9%）。

民眾擁有哪些仍在使用的社群媒體或即時通訊帳號（前五名）



Base：N=1,129，複選（有使用網路者）

臉書與LINE在台灣的市場占有率大



資料來源：2022台灣網路調查，執行時間2022年2月14日至3月15日，加權後數值
樣本數：1941（雙底冊，上網者樣本）

近期網路釣魚探討：
通訊軟體詐騙手法

刑事警察局

機關簡介 新聞活動 通緝令追追追 犯罪預防 刑事鑑定科學 資訊公

偵查第九大隊

偵破「假LINE@帳號送禮券、貼圖」案 竟是網路直播及酒店行銷業者

今年5月臺北市政府警察局中山分局破獲酒店Call客機房詐欺案件，該機房利用LINE通訊軟體假扮酒店小姐，誘騙被害人到酒店消費，再由小姐以「爸死、母病、兄受傷」、「家裡需要錢」等各種名目詐騙金錢。該機房遭警方搜索後，仍有民眾持續在LINE上收到酒店攬客訊息，經本局溯源偵查，發現竟與今年持續發生的假冒官方LINE@帳號贈送禮券、貼圖案件有關。本局偵查第九大隊遂與臺北市政府警察局刑警大隊、中山分局及保二總隊刑警大隊共組專案小組追查，並報請臺中地方檢察署檢察官指揮偵辦。

許多民眾都曾在LINE收到假冒官方帳號的訊息，「全〇福利中心響應父親節活動 領取500元禮券」、「西〇牛排禮券五人份」、「你分享 我請客 陶〇屋雙人份精選套餐券」、「中〇加油金500元」及「點此下載-反應過激的貓貼圖」，聲稱只要加入LINE@帳號為好友即可領取禮券、加油金、免費貼圖等優惠。這些假帳號都是盜用商標LOGO做為大頭貼照片以假亂真，由於是免費的優惠訊息，再搭配母親節、父親節等節慶活動，在短時間內就會有數千甚至上萬人受騙加入好友。警方發現，這些假網站與帳號，是不法人士盜用知名公司商標架設網站，再透過LINE或Facebook等通訊軟體及社群網站，散佈優惠活動的假訊息，實際上都是騙局一場，民眾加入好友後，根本沒有優惠可領取，造成遭盜用商標之全〇、王〇集團、統〇超商、台灣中〇等公司不斷接到民眾客訴，故訴請警方偵辦。

經本局偵九大隊向臺中地方法院聲准搜索票後，兵分三路同步搜索，查獲犯嫌詹嫌等4人，並查扣蘋果筆電一臺等證物，調查後發現這些假冒的官方網站與帳號，竟是不肖網路直播及酒店行銷業者的員工，透過假的官方LINE@帳號詐騙民眾加入好友，過了二、三週之後，可能早已忘記當初有加入假帳號，再將這些帳號更換大頭貼及暱稱，以直播主或酒店小姐的身分，每天向民眾噓寒問暖及分享生活，再聲稱工作受委屈、家庭困難等說詞，要求民眾前往酒店消費或在直播平臺購買禮物贈送，讓不知情的民眾陷入愛情陷阱，藉以賺取不法利益。

刑事警察局提醒民眾，對於網路及LINE群組所傳送的「免費貼圖」或「優惠券」訊息，應仔細分辨LINE@帳號「盾牌顏色」，官方帳號為「綠色」，認證帳號為「藍色」，「灰色」則是一般帳號，若屬知名品牌卻是顯示「灰色」盾牌，民眾就應該提高警覺，避免誤入詐騙陷阱。

中華民國內政部
MINISTRY OF THE INTERIOR, R.O.C. (TAIWAN)

冒用公眾人物LINE詐財 內政部籲勿輕信、多查證

發布日期：111-09-27 11:35 | 單位：警政署

近期多有詐騙集團盜用各地縣長、區長或村里長等公職人員照片及名字，成立Line群組邀請民眾加好友問好，隨後向民眾借錢的情形，內政部次長陳宗彥今(27)日表示，目前桃園市、臺南市、高雄市、南投縣、雲林縣等地均發現類似詐騙手法，刑事警察局已成立專案小組偵辦，初步追查IP來自境外，提醒民眾，收到來路不明訊息借款、募款，謹記防詐秘訣「1聽、2掛、3查證」，以免受騙。

陳宗彥指出，這類「假親友借款」為常見詐欺手法，而近期正值選舉期間，詐騙集團假冒公眾人物的LINE，主動聯繫民眾進行詐騙，已嚴重擾亂社會秩序，呼籲民眾切勿輕信，並撥打165反詐騙諮詢專線查證。另也提醒公眾人物發現個人名義遭冒用成立假Line帳號，除了可通知親友、選民避免受騙外，亦可透過Line官方管道檢舉，保護自己也保護民眾：

1.如何檢舉帳號侵權：https://official-blog-tw.line.me/archives/11978985.html。

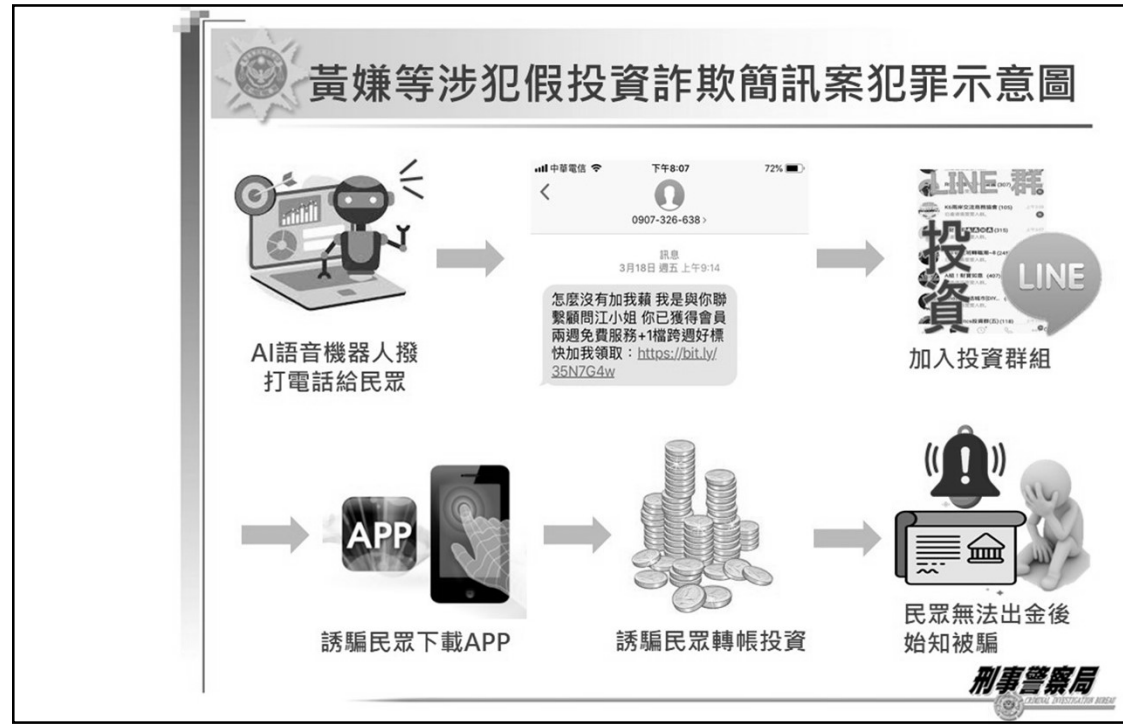
2.如何避免被陌生人加好友：https://official-blog-tw.line.me/archives/9875725.html。

發布日期：111-12-01 更新日期：111-12-05 發布單位：刑事警察局公共關係室

內政部警政署 刑事警察局 CRIMINAL INVESTIGATION BUREAU

詐團也懂AI!新手法發送投資詐欺簡訊，仍遭警搗破

一、偵辦單位：臺灣高雄地方檢察署、刑事警察局偵查第九大隊、高雄市政府警察局、臺北市政府警察局、臺中市政府警察局
二、查獲時間：111年9月27日
三、查獲地點：高雄市、臺中市
四、查獲嫌犯：黃○○（男、40歲、高雄人）、蘇○○(男、28歲、高雄人)等2人。
五、查獲贓證物：公司大小章、租用申請書、匯款單影本、後臺詐騙簡訊電磁紀錄、語音講稿等證物。
六、案情摘要及偵辦過程：
(一)詐欺集團假冒金控或知名投顧公司濫發詐欺簡訊，誘使民眾加LINE好友，再鼓吹加入LINE投資群組，群組內犯嫌扮演投顧老師及成員，以投資話術詐騙被害人，因投資詐騙簡訊為詐欺案件前置行為，本局偵查第九大隊接獲情資，即針對是類簡訊擴大偵辦。
(二)經追查發現犯嫌以投顧企業社名義向電信公司取得數百個電信門號並申請大量企業簡訊服務，除自己公司外，亦接受其他詐欺集團委託發送投資詐欺簡訊，其儲值簡訊費用達新臺幣1億元以上，初估已發送簡訊量達6千萬則，平均每月達6百多萬則。經本局進一步追查，發現犯嫌為增加簡訊命中率，竟利用科技公司之AI語音機器人服務，隨機向民眾撥打語音電話，再從民眾與AI語音機器人對話的口氣，篩選對投資有興趣的民眾傳送簡訊，民眾上鉤後再指導下載專用APP，並匯5千元成為會員，體驗七天5萬元投資額度，再以投資獲利為誘餌，鼓吹民眾加碼投資，致民眾受騙損失慘重。
(三)經專案小組報請臺灣高雄地方檢察署指揮，於今年九月分別至高雄、臺中等地執行搜索，當場查獲犯嫌黃、蘇2人到案，查扣手機4隻、公司大小章、租用申請書、匯款單影本、語音講稿、後臺詐騙簡訊電磁紀錄等證物，阻斷發訊門號155門，凍結儲值金額9百餘萬元，全案依詐欺等罪移請高雄地檢署偵辦。
(四)依據本局165反詐欺專線統計，自本局執行跨部會打擊詐欺簡訊專案後，因詐騙簡訊被害案件已從111年8月的1049件，逐步下降至10月僅102件，下降幅度高達90%，本局將持續針對是類詐欺簡訊平臺進行掃蕩，從源頭阻詐。本局在此呼籲，民眾投資應慎選合法投資管道，勿輕信來源不明的投資訊息，若發現疑似詐欺的投資簡訊，除可善用「165全民防騙網」每周公告的「詐騙LINE ID」查證，另可撥打165反詐騙諮詢專線求證。



金融監督管理委員會 Financial Supervisory Commission
Banking Bureau 銀行局

https://www.banking.gov.tw/ch/home.jsp?id=125&parentpath=0,555&mcustomize=FscSearch_RelatedLink.jsp&type=1

經 Google 技術強化

回首頁 > 金融機構

金融機構

金融控股公司 | 本國銀行 | 票券商 | 信用合作社 | 外銀在臺辦事處

目前網址 **有** – 只有：
- 合作金庫銀行 www.tcb-bank.com.tw
- 樂天國際銀行 www.rakuten-bank.com.tw
- 王道銀行 www.o-bank.com

目前網址 **沒有 .tw** 共有：
- 台北富邦銀行 www.fubon.com
- 中國信託銀行 www.ctbcbank.com
- 渣打銀行 www.sc.com
- 永豐銀行 bank.sinopac.com
- 凱基銀行 www.kgibank.com
- 彰化銀行 www.bankchb.com

內政部警政署 刑事警察局 CRIMINAL INVESTIGATION BUREAU

發布日期：112-03-11 更新日期：112-03-12 發布單位：刑事警察局公共關係室

投資千萬元全打水漂 官方市集APP亦不可輕信

民眾S姓女子因加入自稱「股票分析師助理」之投資LINE群組，群組內老師「蔣明誠」每日分析股票走勢、政治、國際經濟、比特幣，後來老師推薦S姓女子從APP Store下載「BTMIN GT」APP，並以「陌生個人銀行帳號」供S姓女子匯款儲值，因為是在官方市集下載， S姓女子不疑有他陸續投入上千萬元。

操作幾次之後，向LINE名稱「比特幣操作小姐」申請出金，初期確實有成功提領，但平臺卻在今年1月初要求使用者「提供與身分證相符之銀行帳戶」、「繳付帳戶內10%金額驗證身分後才能出金」等，S姓女子因此到處借錢，直到銀行行員察覺有異並通報警方到場苦口婆心勸說，S姓女子才驚覺被騙。

165反詐騙專線提醒，「雖然官方市集下載的應用程式經過初步審核上架，但也可能被利用作為詐騙」，民眾應小心查證避免落入詐騙圈套，並在下載APP前參考其他使用者的評價，以免受騙。事實上，只要民眾每次投資入金的帳戶都是「陌生個人銀行帳號」，極有可能是詐騙集團的人頭帳戶。

警方呼籲，各類投資行為應透過主管機關金管會核准的機構或公司，方能維護自身投資權益，如有陌生人或網友以高報酬、穩賺不賠等話術招募投資，請務必提高警覺，並撥打金管會反詐騙諮詢專線（02-2737-3434）確認訊息來源真實性，或至國際投資警訊專區（http://web.twsa.org.tw/alert/）查證；如有可疑詐騙情資，亦可透過「165全民防騙官網或警政服務APP」，填入「姓名、連絡電話、註解訊息（將訊息複製貼上）及驗證碼等資訊」，再將訊息內容截圖上傳後送出，即可快速完成詐騙訊息的檢舉，以利警方後續追查不法，亦可前往鄰近分局、分駐（派出）所，由員警受理後進行轉報及協助。

https://www.fisac.tw

近期網路釣魚探討：
電子支付詐騙手法

發稿時間	2019/7/26 下午 02:47:52
查獲地點	新○市、臺○市
查獲嫌犯	蕭○○、李○○、葉○○、吳○○、陳○○等5人
查獲贓證物	行動電話3具、電腦主機1臺

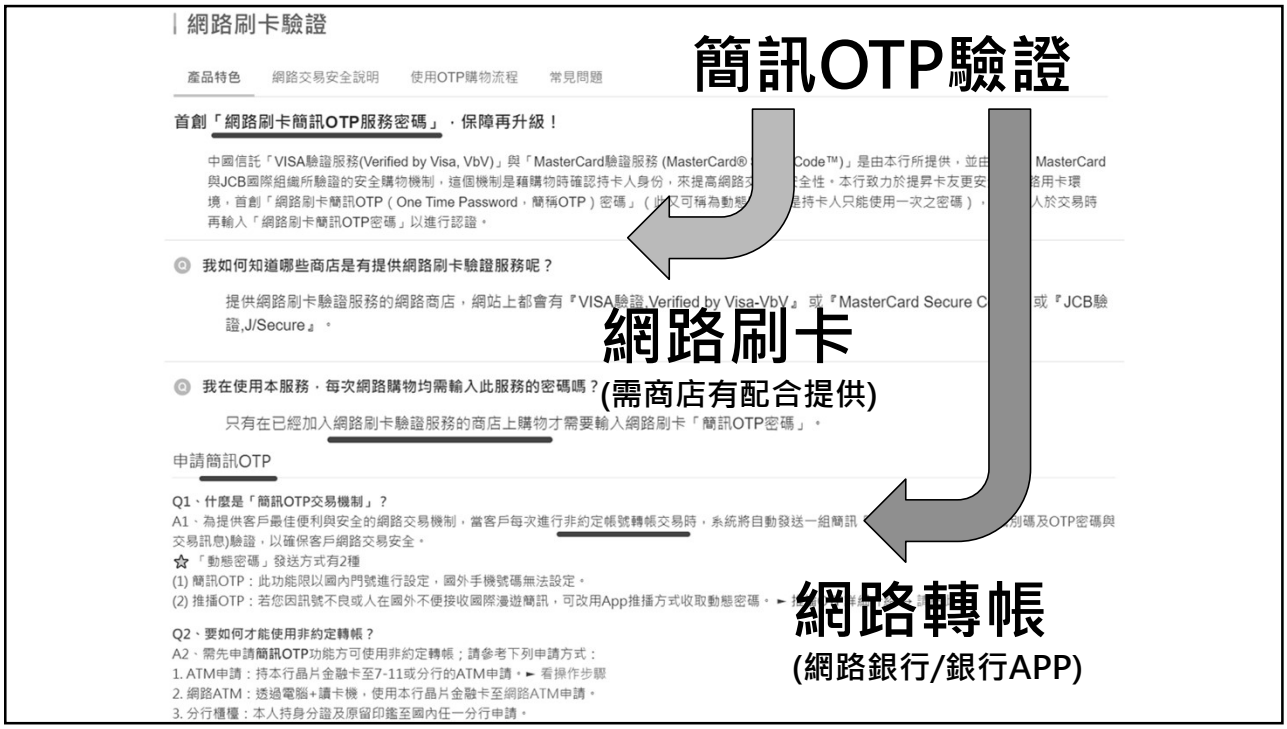
案情摘要

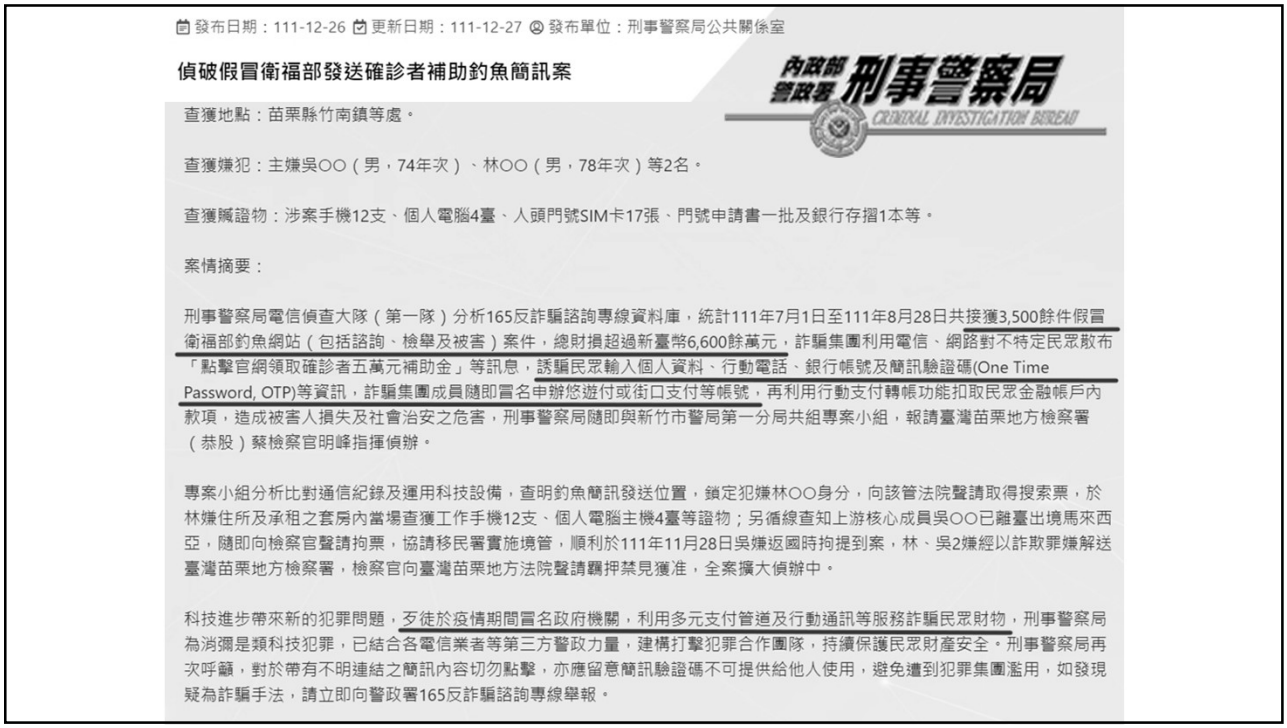
(一)刑事警察局偵查第一大隊(第一隊)接獲國內知名電商報案稱公司旗下電子購物商城網站於107年3月起，即發生多起使用信用卡刷卡商品訂購成功且出貨後，然而國內信用卡持卡人否認交易，且信用卡公司拒付款項或將已支付款項收回，致生該公司損失約新臺幣(下同)60餘萬元，偵查期間，偵查第一大隊(第二隊)也接獲某被害公司報案，稱有多名用戶於網路門市上申辦門號、購買高價手機，並以信用卡付款，然卻收到信用卡持卡人否認交易，致該被害公司損失新臺幣約80萬元，即共組專案小組偵辦，。

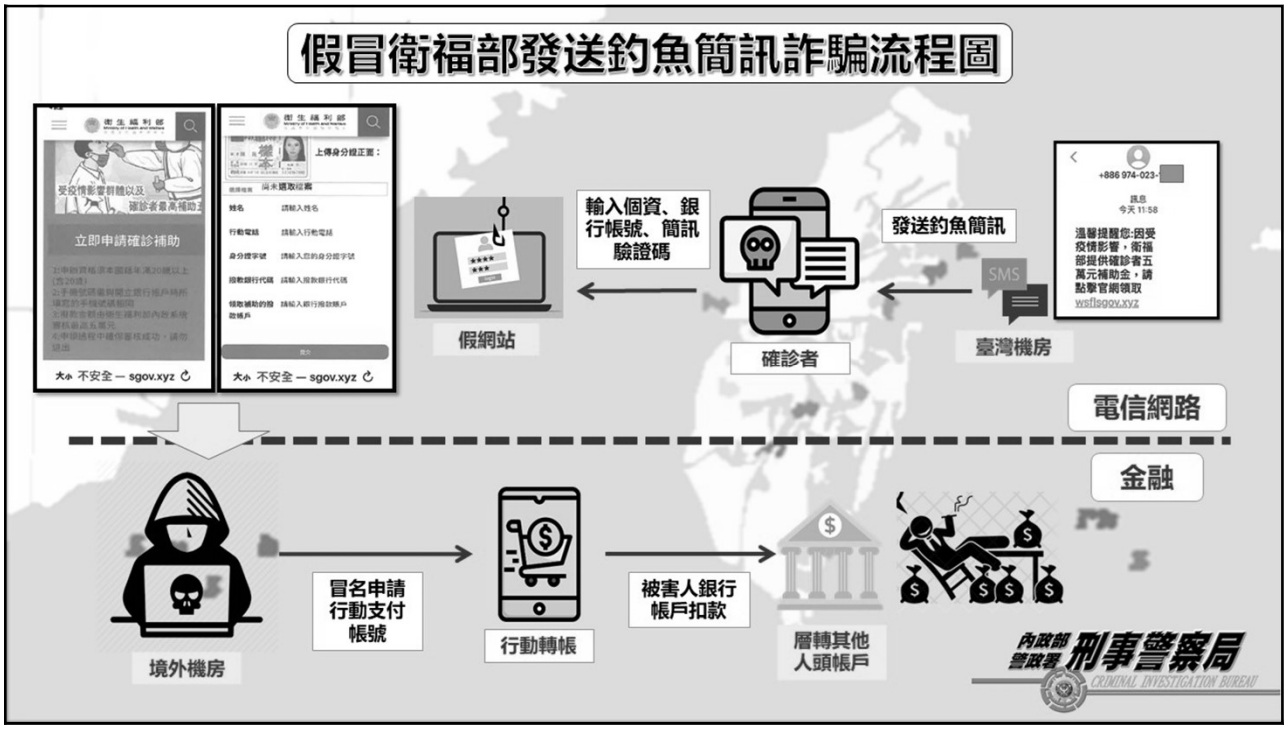
(二)專案小組多月追查，偵查發現國內應該有2團信用卡盜刷集團從事不法犯罪，但都是向國外網站購買信用卡資訊後，至國內電商及電信系統商進行盜刷，利用部分網路商家刷卡付款無經過3D驗證(簡訊驗證)機制，以及部分第三方支付APP綁定信用卡無須驗證之漏洞，大肆盜刷信用卡購買高單價商品變賣獲取暴利，盜刷購買多為高階iphone手機、3C產品、保養品等易銷贓商品。

(三)案經數月偵查及蒐證，見時機成熟，發動2波查緝，刑事警察局偵查第一大隊(第一隊)會同臺北市政府警察局南港分局分別於7月12日發動查緝，查獲主嫌蕭○○等5人到案，偵查第一大隊(第二隊)於7月25日會同臺北市政府警察局文山第一分局、臺北市政府警察局刑事警察大隊偵查第四隊等單位，查緝主嫌陳○○等9人到案，訊後全案將上述2團計犯嫌14人依詐欺罪嫌移送臺灣新北地方檢察署偵辦。

(四)近來手機結合金融卡的支付型態越來越盛行，許多民眾手機門號皆有綁定信用卡卡號，警方呼籲民眾，刷卡消費時勿讓信用卡離開視線避免遭不法之徒竊取信用卡卡號其他個資，為及時發現信用卡盜刷避免損失擴大，可向發卡銀行申請簡訊通知刷卡服務，同時養成對帳習慣，發現帳單上有不明交易，應隨時向銀行確認，保障自己的權益。警方也呼籲商家應該向銀行申請3D認證，才可保障信用卡交


網路刷卡驗證
產品特色
網路交易安全說明
使用OTP購物流程
常見問題
首創「網路刷卡簡訊OTP服務密碼」，保障再升級！
中國信託「VISA驗證服務(Verified by Visa, VbV)」與「MasterCard驗證服務 (MasterCard®
Code™)」是由本行所提供，並由
MasterCard
與JCB國際組織所驗證的安全購物機制，這個機制是藉購物時確認持卡人身份，來提高網路交
全性，本行致力於提昇卡友更安
路用卡環
境，首創「網路刷卡簡訊OTP（One Time Password，簡稱OTP）密碼」（此又可稱為動態
是持卡人只能使用一次之密碼），
人於交易時
再輸入「網路刷卡簡訊OTP密碼」以進行認證。
我如何知道哪些商店是有提供網路刷卡驗證服務呢？
提供網路刷卡驗證服務的網路商店，網站上都會有『VISA驗證 Verified by Visa-VbV』或『MasterCard Secure C
或『JCB驗
證,J/Secure』。
我在使用本服務，每次網路購物均需輸入此服務的密碼嗎？
只有在已經加入網路刷卡驗證服務的商店上購物才需要輸入網路刷卡「簡訊OTP密碼」。
申請簡訊OTP
Q1、什麼是「簡訊OTP交易機制」？
A1、為提供客戶最佳便利與安全的網路交易機制，當客戶每次進行非約定帳號轉帳交易時，系統將自動發送一組簡訊
別碼及OTP密碼與
交易訊息)驗證，以確保客戶網路交易安全。
☆「動態密碼」發送方式有2種
(1) 簡訊OTP：此功能限以國內門號進行設定，國外手機號碼無法設定。
(2) 推播OTP：若您因訊號不良或人在國外不便接收國際漫遊簡訊，可改用App推播方式收取動態密碼。►
Q2、要如何才能使用非約定轉帳？
A2、需先申請簡訊OTP功能方可使用非約定轉帳；請參考下列申請方式：
1. ATM申請：持本行晶片金融卡至7-11或分行的ATM申請。► 看操作步驟
2. 網路ATM：透過電腦+讀卡機，使用本行晶片金融卡至網路ATM申請。
3. 分行櫃檯：本人持身分證及原留印鑑至國內任一分行申請。
簡訊OTP驗證
網路刷卡
(需商店有配合提供)
網路轉帳
(網路銀行/銀行APP)


發布日期：111-12-26 更新日期：111-12-27 發布單位：刑事警察局公共關係室
偵破假冒衛福部發送確診者補助釣魚簡訊案
內政部警政署 刑事警察局 CRIMINAL INVESTIGATION BUREAU
查獲地點：苗栗縣竹南鎮等處。
查獲嫌犯：主嫌吳○○（男，74年次）、林○○（男，78年次）等2名。
查獲贓證物：涉案手機12支、個人電腦4臺、人頭門號SIM卡17張、門號申請書一批及銀行存摺1本等。
案情摘要：
刑事警察局電信偵查大隊（第一隊）分析165反詐騙諮詢專線資料庫，統計111年7月1日至111年8月28日共接獲3,500餘件假冒衛福部釣魚網站（包括諮詢、檢舉及被害）案件，總財損超過新臺幣6,600餘萬元，詐騙集團利用電信、網路對不特定民眾散布「點擊官網領取確診者五萬元補助金」等訊息，誘騙民眾輸入個人資料、行動電話、銀行帳號及簡訊驗證碼(One Time Password, OTP)等資訊，詐騙集團成員隨即冒名申辦悠遊付或街口支付等帳號，再利用行動支付轉帳功能扣取民眾金融帳戶內款項，造成被害人損失及社會治安之危害，刑事警察局隨即與新竹市警局第一分局共組專案小組，報請臺灣苗栗地方檢察署（恭殷）蔡檢察官明峰指揮偵辦。
專案小組分析比對通信紀錄及運用科技設備，查明釣魚簡訊發送位置，鎖定犯嫌林○○身分，向該管法院聲請取得搜索票，於林嫌住所及承租之套房內當場查獲工作手機12支、個人電腦主機4臺等證物；另循線查知上游核心成員吳○○已離臺出境馬來西亞，隨即向檢察官聲請拘票，協請移民署實施境管，順利於111年11月28日吳嫌返國時拘提到案，林、吳2嫌經以詐欺罪嫌解送臺灣苗栗地方檢察署，檢察官向臺灣苗栗地方法院聲請羈押禁見獲准，全案擴大偵辦中。
科技進步帶來新的犯罪問題，歹徒於疫情期間冒名政府機關，利用多元支付管道及行動通訊等服務詐騙民眾財物，刑事警察局為消彌是類科技犯罪，已結合各電信業者等第三方警政力量，建構打擊犯罪合作團隊，持續保護民眾財產安全。刑事警察局再次呼籲，對於帶有不明連結之簡訊內容切勿點擊，亦應留意簡訊驗證碼不可提供給他人使用，避免遭到犯罪集團濫用，如發現疑為詐騙手法，請立即向警政署165反詐騙諮詢專線舉報。



銀行 APP & 綁定銀行帳戶 & 綁定信用卡

- 完全不使用銀行APP。(用網頁版的網路銀行查詢)
- 電子錢包 → 綁定銀行帳戶
  - 申辦一個**只存放小額金錢**(例如：5000元)的銀行帳戶 → 綁定在網路消費
  - 申辦另一個存放大筆金額(例如：利率/利息較高)的銀行帳戶 → 不在網路上使用
- 電子支付、購物/外送APP → 綁定信用卡
  - 申辦一張**額度較小**(例如：5000元)的信用卡 → 綁定在網路消費
  - 申辦一張額度較大的信用卡 → 只在實體門市消費

帳號密碼的新風險：
多因子認證 (MFA)

110年民眾通報高風險賣場排名

高風險賣場報案排名
HITO本舖：121件
GOMAJI：107件
Booking.com：102件
DR情趣：95件
Check2check：94件

統計110年1至3月

高風險賣場報案排名
誠品網路書店：310件
金石堂網路書店：175件
萬年東海模型：147件
婕洛妮絲：144件
Booking.com：119件

統計110年4至6月止

高風險賣場報案排名
東森購物：330件
誠品網路書店：308件
HITO本舖：128件
蝦皮購物：128件
CACO：96件

統計110年7至9月止

高風險賣場報案排名
東森購物：453件
誠品書店：322件
蝦皮購物：220件
CACO：179件
婕洛妮絲：136件

統計110年10至12月止

111年民眾通報高風險賣場排名

高風險賣場報案排名
東森購物：529件
誠品書局：240件
遠傳friDay購物：143件
蝦皮購物：125件
金石堂：90件

統計111年1至3月止

高風險賣場排名
博客來網路書店：2725件
迪卡儂：477件
誠品網路書店：252件
遠傳friDay購物：162件
蝦皮購物：119件

統計111年4至6月止

高風險賣場排名
博客來網路書店：905件
旋轉拍賣：529件
鞋全家福：277件
生活市集：220件
迪卡儂：191件

統計111年7至9月止

高風險賣場報案排名
旋轉拍賣：1225件
蝦皮拍賣：500件
生活市集：355件
順發3C：353件
ONE BOY：342件

統計111年10至12月止

109～111年全年度民眾通報高風險賣場排名

高風險賣場報案排名
MOMO：383件
小三美日：283件
讀冊生活：275件
486團購網：242件
HITO本舖：208件

統計109年1至12月止

高風險賣場報案排名
誠品書店：940件
東森購物：868件
蝦皮購物：500件
婕洛妮絲：358件
金石堂：324件

統計110年1至12月止

高風險賣場報案排名
博客來網路書店：3773件
旋轉拍賣：1764件
蝦皮拍賣：931件
誠品書局：823件
迪卡儂：668件

統計111年1至12月止

內政部警政署 刑事警察局 CRIMINAL INVESTIGATION BUREAU

發布日期：112-03-12 更新日期：112-03-12 發布單位：刑事警察局公共關係室

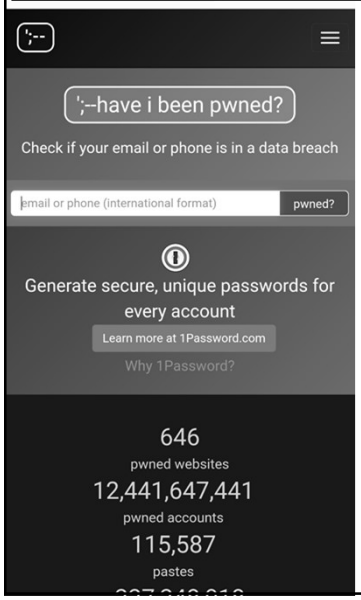
蝦皮、旋轉拍賣平台用戶淪為釣魚網站攻擊目標，刑事局提醒民眾網路交易應多小心

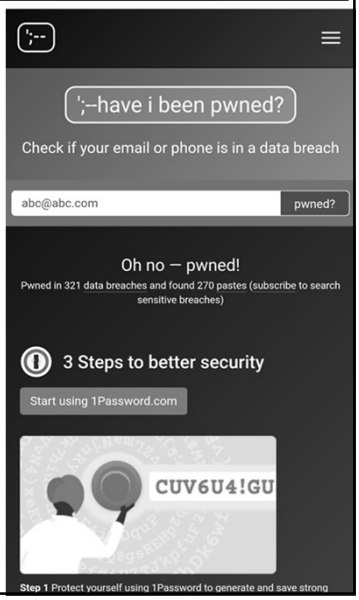
據刑事局分析165反詐騙諮詢專線民眾報案資料發現，近期駭客以假冒「蝦皮拍賣」、「旋轉拍賣」等C2C交易平台網頁進行釣魚網站攻擊，主要係為盜取大量民眾網路交易個人資料，然後進行解除分期付款詐騙。

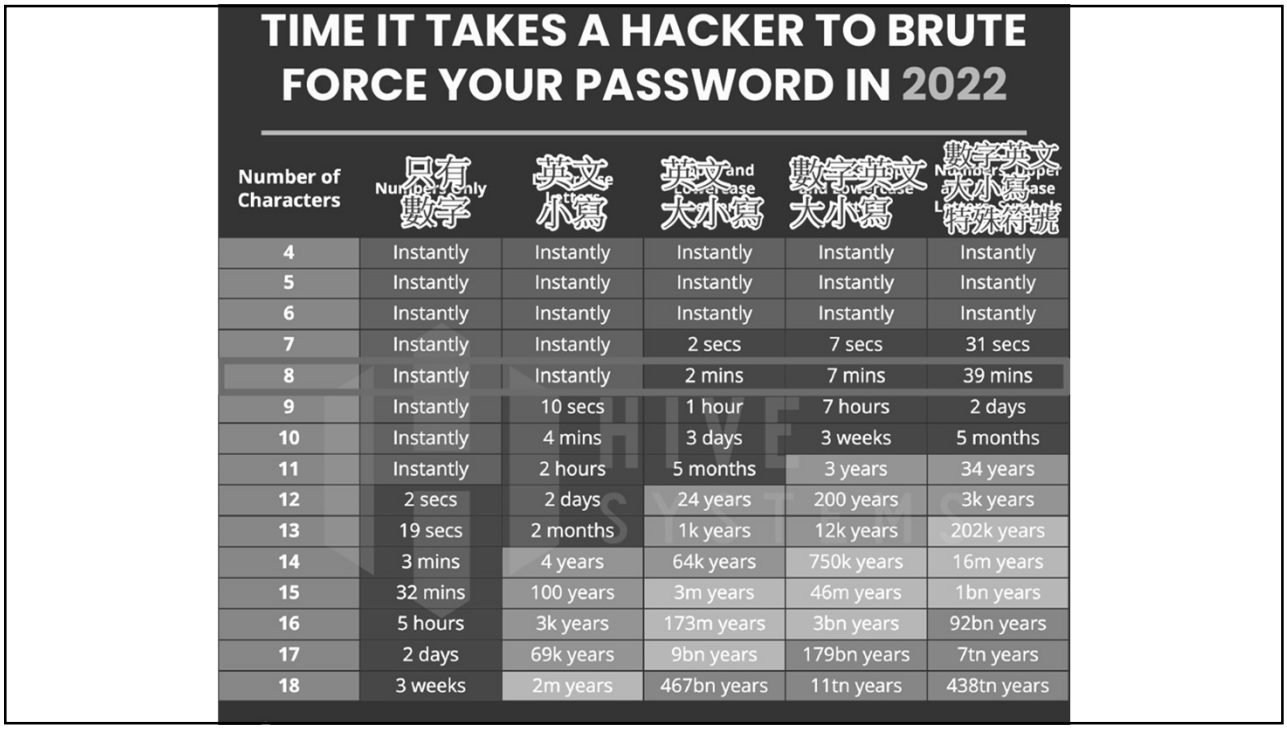
由於「蝦皮拍賣」、「旋轉拍賣」等係屬新加坡外商公司所有，在國內僅少數行政管理人員，更無設置專業資安團隊協助民眾帳號、密碼遭到入侵後防護，統計上述2網路平台迄今已蟬聯5週高風險賣場第1名、第2名，業由刑事局依違反個資法函送目的事業主管機關(數位發展部)查處中，並於去年12月底由主管機關實施行政檢查要求限期改善，惟迄今均未有具體作為，因此特別呼籲民眾應慎選賣場進行購物，以免造成財物損害。

近年來各大購物平臺發生個資外洩事件頻傳，詐騙集團利用駭客竊得國人交易個資(購買時間、商品名稱、金額及付款方式等)，並偽冒公司客服人員及解除分期付款詐術手段，誘騙民眾至ATM(或網路銀行)進行轉帳詐騙，有鑒於此，本局除定期公布高風險賣場，提醒消費者注意受騙外，亦主動針對疑似個資外洩電商進行訪視與入侵追查，情節嚴重者依「個人資料保護法」及「行政院及所屬各機關落實個人資料保護聯繫作業要點」通報目的事業主管機關裁處，統計111年6月至112年2月為止，已函送數位發展部、衛生福利部、交通部、教育部、經濟部、文化部、通傳會等7部會共計上百家疑似外洩個資之電商，但發動行政檢查要求改善者僅約占少數1成，且近1年來均無裁罰紀錄，對於罔顧資安之不肖電商業者並無約束力；反觀，個資外洩造成的解除分期付款詐騙案，光2個月發生件數可高達近千件，財損超過新臺幣1億多元，與電商投資之資安成本大相逕庭，雖行政院3月2日已定調未來個資法修法及提高裁罰額度，但在個資法尚未修法之前，刑事局亦持續促請各目的事業主管機關共同協力監督電商，並加速違規業者行政裁罰以改善資安，共同防堵詐騙事件發生。

https://haveibeenpwned.com







TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	只有數字 Numbers only	英文小寫 Lowercase letters	英文大小寫 Upper and lowercase letters	數字英文大小寫 Numbers and upper and lowercase letters	數字英文大小寫特殊符號 Numbers, upper and lowercase letters, symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

密碼設定

- 需包含英文大小寫、數字及符號。
- 密碼需要 8 個字(12~16 個字)以上。
- 不可以另外寫下 或 存在電腦檔案裏。

帳號密碼的新風險：
無密碼身分識別(FIDO)

雜亂無章的密碼組合不僅不安全又痛苦...

我總是記不住密碼？
重設時的密碼規則又限制很多。

為什麼每個網站都有不同密碼?

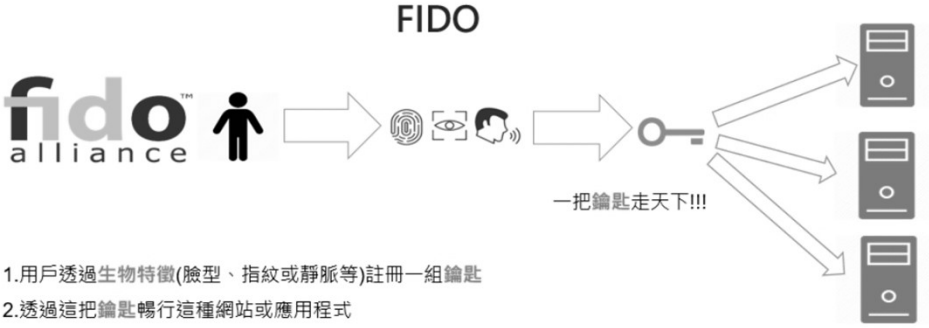
複雜到自己都記不住還是被盜用...

什麼是 FIDO？

FIDO 全稱為 Fast IDentity Online。

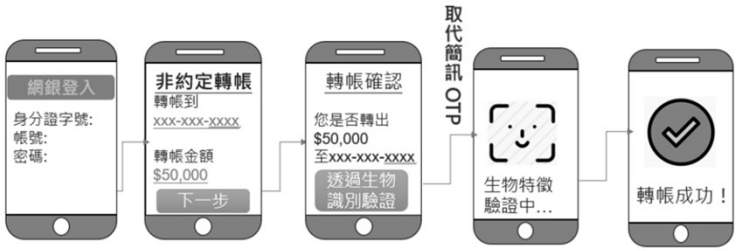
是一種為了將跨網站、應用等多組密碼整合為同一組快速且安全的登入方式的技術標準。

FIDO



1.用戶透過生物特徵(臉型、指紋或靜脈等)註冊一組鑰匙
2.透過這把鑰匙暢行這種網站或應用程式

流程示意 – 以 FIDO ID取代簡訊OTP交易驗證



流程示意 – 以 FIDO ID進行憑證數位簽章

https://fido.moi.gov.tw


瀏覽人數：4887200
En
APP
關於我們
功能教學
最新消息
公開資料
檔案下載
需用機關專區
您在政府網站上的通行證
只要註冊行動自然人憑證會員，如同取得在政府網站的行動通行證，可以登入多個政府網站來取得您的個人服務。
免插卡，透過手機APP快速登入多項服務
過去使用政府網路服務必須仰賴自然人憑證或申請帳密，行動自然人憑證只要透過APP驗證身分，即可使用眾多政府服務。
結合生物特徵驗證，避免身分被冒用、安全更升級
行動自然人憑證服務採生物特徵識別方式驗證身分，手機即使遺失也不用擔心身分被冒用，安全更有保障。


瀏覽人數：4887086
En
自然人憑證
下載APP
關於我們
功能教學
最新消息
公開資料
檔案下載
需用機關專區
請與說明
腦作業系統與行動系統說明
冊問題
定問題
用說明
全性說明
Q1 生物特徵辨識是否存在風險？
Ans 各種登入及驗證機制都存在風險，說明如下：(1)關於生物特徵的存取：本服務並不會存取您的生物特徵值。登入進行生物特徵驗證時，是利用您原本儲存於行動裝置(手機或平板)的臉部或指紋，確認為本人後才啟動後續的驗證機制，加強您個人隱私的安全性。(2)只有在您的行動裝置本身存取本人以外其他人的生物特徵時，才有可能被其他人登入，因此無論是使用個人的行動裝置或任何設備，為避免個人資料被竊取，做好個人資料保護及安全是每位民眾使用本服務的義務。
Q2 假設其他人想使用我的帳號去綁定行動自然人憑證，請問是可行的嗎?
Ans 不行，因經過您本人授權同意給他人使用自己的帳號，故後續的認證和交易應自行負責，因此需請審慎考慮。
Q3 請問生物特徵識別(如指紋、臉)有沒有效期？
Ans 生物特徵資料為儲存於行動裝置(手機或平板)內，以使用者綁定之行動裝置設定為主，如使用者已經將行動裝置上建立的生物特徵移除，則無法透過本服務進行身分識別，另當行動裝置壞掉或更換了，亦無法使用本服務。

帳號密碼的新風險：
深偽技術(Deepfake)

什麼是 深偽技術 (Deepfake)？

- 深偽技術 (Deepfake) 又稱深度偽造，是深度學習 (deep learning) 和偽造 (fake) 的混和名詞，指將已有的圖像或影片合成疊加至目標圖像或影片上進行偽造的技術。
- 一種肉眼難辨的修圖或者影片合成的技術。
- 目前常見於換臉偽造的手法，主要是透過交換兩張圖像的人臉達到偽造身分的目的。
- 現階段換臉偽造和表情偽造，已經可以結合語音偽造技術，達到完全偽裝的手法。

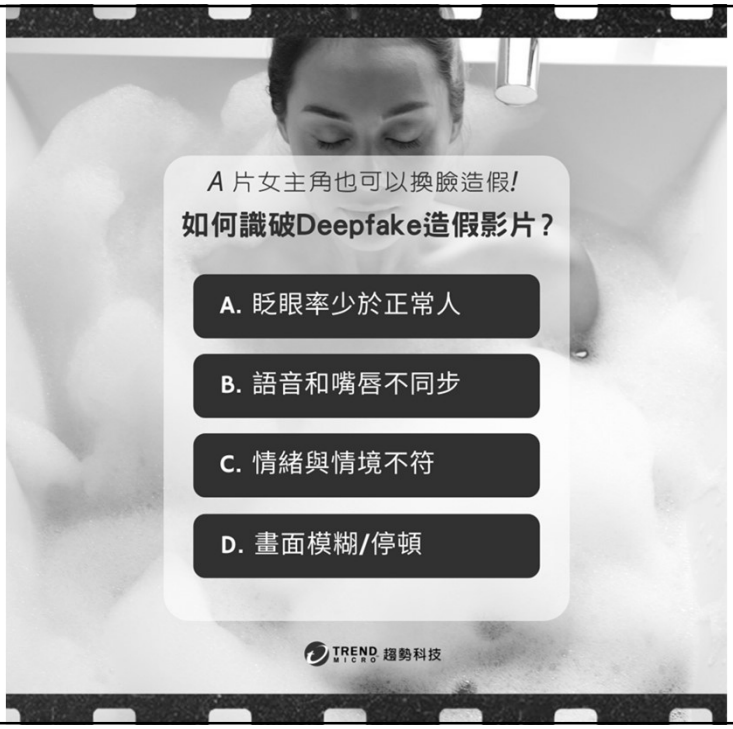
https://chat.openai.com

DeepFake 的危害：

圖像、影片、聲音都可以偽造

- 移花接木色情影片
- 偽造名人傳播假訊息
- 破解人臉辨識盜領存款

成為一種非常不容易辨識的社交工程手法以及詐騙工具。



常見資安事件宣導：
物聯網(IoT)與監視攝影機

何謂物聯網

- 物聯網(Internet of Things，IoT)是一個基於網際網路、傳統電信等資訊，讓所有能夠被獨立賦予 IP 的電子物品實現相互聯絡的網路。
- 物聯網的核心和基礎依然是網際網路。但未來可能需要一系列技術升級才能滿足物聯網的需求，例如：IPv6、RFID、NFC 等。
- 維基百科：
- https://zh.wikipedia.org/wiki/物聯網

http://www.insecam.org/cn/bycountry/TW/

物聯網攻擊案例

案情提要

- 機關某廠牌監視器發現遭植入Mirai家族惡意程式，並至中繼站報到
- 經調查該監視器遭揭漏存在存在路徑走訪(Path Traversal)、緩衝區溢位(Buffer Overflow)及命令注入(Command Injection)漏洞等安全性漏洞

【機關處置方式】

–重置設備、變更監視器預設帳號密碼，並更新韌體版本至最新版本

防護建議

- 應評估設備供外部連線之必要性
- 設置新購資訊設備應立即變更預設帳號密碼
- 定期檢視並更新設備系統/韌體版本

18

物聯網設備檢測共同發現事項

1. 設備的管理介面、Telnet及SNMP服務使用預設帳號密碼，恐有資訊外洩與遭受入侵疑慮
3. 設備管理介面未設定密碼錯誤嘗試次數，容易遭受暴力破解攻擊
2. 軟/韌體、作業系統及相關應用程式存在CVSS v3高於7分(含)之CVE漏洞

使用者　　物聯網設備

改善建議

發現事項1與2同110年

1. 設備管理者應禁止管理介面使用預設帳號密碼，並關閉非必要服務
2. 設備管理者定期針對物聯網設備韌體與後端服器主機作業系統進行更新
3. 設備管理者應設定與啟用密碼錯誤嘗試次數，避免遭受暴力破解攻擊

52

常見資安事件宣導：
郵件社交工程

郵件社交工程攻擊之定義

- 利用人性弱點、人際交往或互動特性所發展出來的一種攻擊方法
- 早期社交工程是使用電話或其他非網路方式來詢問個人資料，而目前社交工程大都是利用電子郵件或網頁來進行攻擊
- 透過電子郵件進行攻擊之常見手法
  - 假冒寄件者
  - 使用與業務相關或令人感興趣的郵件內容
  - 含有惡意程式的附件或連結
  - 利用應用程式之弱點(包括零時差攻擊)

郵件社交工程的手法

- 當收件人
- 開啟惡意電子郵件或
- 預覽惡意電子郵件或
- 點閱惡意電子郵件所附超連結或
- 點閱惡意電子郵件所附件檔案時，
- 即留下紀錄，或者感染病毒

- 並且可以統計
- 該惡意電子郵件的開啟率及
- 該惡意電子郵件的點閱率做為下一次詐騙之依據。

郵件社交工程
真實攻擊手法

twcert/cc

首頁 / 資安宣導 / 資訊安全宣導

近期偽冒政府機關網域發送勒索用戶之詐騙郵件

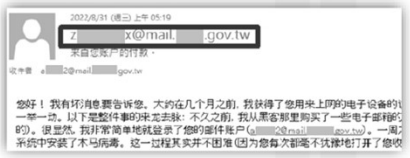
2022-08-30

本中心近期接獲民眾收到勒索郵件的通報，該郵件來源為駭客偽冒政府機關網域發送詐騙郵件。郵件內宣稱駭客已取得用戶電子郵件的訪問權限、於用戶的電子設備植入惡意軟體，並取得用戶所有的通訊與活動紀錄。接著表明擁有用戶的私密影片，若不希望影片外流必須支付特定數量的比特幣，否則將會公開用戶的私密影片至其親友。

提醒民眾，收到此類詐騙郵件請勿匯款，建議先聯繫相關單位進行求證，或是至TWCERT/CC官網進行通報。

偽冒機關帳號散布惡意電郵案例

- 駭客利用政府機關電子郵件伺服器未設定寄件者原則架構(SPF)，大規模偽冒政府機關人員電子郵件帳號，發送大量惡意勒索電子郵件進行社交工程攻擊
  - 111年9月偵測發現，遭駭客偽冒之政府機關，共計87個政府機關、117機關域名未完善SPF設定



未設定SPF之機關責任等級分布	
A級機關	6
B級機關	27
C級機關	38
D級機關	13
其他	3(資安法尚未列管)

防護建議

- 建議可參考寄件者原則架構(SPF)設定，完善郵件安全防護，避免機關電子郵件帳號遭偽冒利用

21

使用者防護停看聽(1)

- **停 – 使用任何電子郵件軟體前，必須先確認**
  - 執行各種作業系統、應用軟體設定更新
    - Windows Update
    - Office Update
    - Internet Explorer 安全性設定
  - 必須安裝防毒軟體，並確實更新病毒碼
  - 收信軟體安全性設定
    - 如果可行的話以純文字模式開啟郵件
    - 必須取消郵件預覽功能
  - 防止垃圾郵件
    - 設定過濾垃圾郵件機制
  - 啟用個人防火牆

使用者防護停看聽(2)

- **看 –** 開啟電子郵件前應先依序檢視：

  (1)、【寄件者】的信箱來源

  (2)、【郵件主旨】是否與公務相關

  (3)、【附加檔案】不要直接點選打開，應另存新檔掃毒。

  ☺【寄件者】或【郵件主旨】與公務無關者，建議應立即刪除，連預覽都不要開啟郵件。

使用者防護停看聽(3)

- **聽 – 若懷疑郵件來源，必須進行確認**
  - 透過 電話 或 LINE 或 電子郵件 再次向寄件人 **確認**郵件真偽。

資安法規摘要：
個人資料保護法(個資法)

什麼是個人資料？

- 個人資料是一種可以讓大家更加了解我的資訊。

WHO	費歐娜，女生
WHEN	今年17歲
WHAT	1. 家中有爸爸、媽媽和我 2. 遠的要命王國的公主 3. 身高120公分,體重40公斤
HOW	電話:0800-000-000 地址:美國、夢工廠

第 2 條　本法用詞，定義如下：

一、個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

二、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。

三、蒐集：指以任何方式取得個人資料。

四、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。

五、利用：指將蒐集之個人資料為處理以外之使用。

六、國際傳輸：指將個人資料作跨國（境）之處理或利用。

七、公務機關：指依法行使公權力之中央或地方機關或行政法人。

八、非公務機關：指前款以外之自然人、法人或其他團體。

九、當事人：指個人資料之本人。

發布日期：110-07-23 更新日期：110-07-23 發布單位：刑事警察局公共關係室

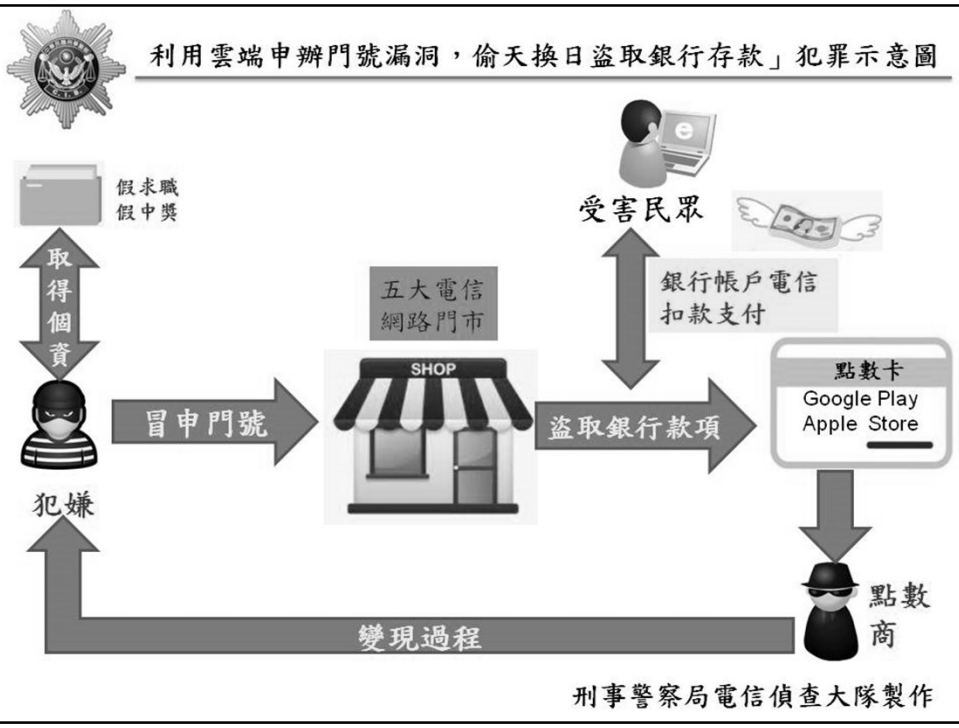
首見利用雲端申辦門號漏洞 偷天換日盜取銀行存款

一、偵辦單位：本局電信偵查大隊(第一隊)、新竹市警察局第一分局。
二、查獲時間：110年7月16日。
三、查獲地點：臺北市大同區。
四、查獲嫌犯：
張○○(男，64年次)、許○○(男，84年次)、
陳○○(男，87年次)、柯○○(男，75年次)、
孔○○(男，58年次)、張○○(男，67年次)、
楊○○(男，86年次)、陳○○(男，88年次)、
陳○○(男，76年次)
伍、查獲贓證物：手機、SIM卡及雲端硬碟資料(民眾雙證件及金融帳戶影本)等電磁紀錄。
六、案情摘要：

本局109年6月起獲報有民眾指稱銀行帳號存款遭不明扣款購買遊戲點數，事後發現證件遭他人偽造申辦人頭門號進行電信代收扣款，隔空取物之特殊犯罪手法令人費解，被害人數超過160餘人及高達新臺幣200餘萬元財損。本局電信偵查大隊與新竹市警察局第一分局共組專案小組，循線擴大追查。

專案小組先查獲張姓主嫌到案後，發現犯嫌取得被害人銀行帳號、身分證等證件，然後以偽造證件上傳各電信業者線上門市，由於業者僅審查身分證號及換發日期，致犯嫌順利通過認證，其後透過物流寄送門號至指定超商取件，再透過電信小額付費詐買GooglePlay、AppleStore虛擬點數，最後與許姓遊戲點數商等8名共犯再轉售予不知情民眾牟利變現，經專案小組數月追查之下，順利在臺北市、新北市、臺中市等地緝捕共犯8人歸案，全案依法移送臺灣士林地方檢察署偵辦。

電信門號近年運用在社群網站認證、網路拍賣、第三方支付、報稅及防疫簡訊認證等領域已具備類實名角色，電信業者審查機制若出現漏洞，前述服務易遭人利用施行詐騙。本局在此呼籲民眾勿聽信來路不明的假求職、假中獎等情節，更不可擅自將個人證件、銀行存摺提供給第三人，避免銀行帳號遭盜用，對於疑似詐騙訊息可撥打165反詐騙諮詢專線查證，才能保障財產安全。



結論

- 近期網路釣魚探討：
  - 通訊軟體詐騙手法
  - 簡訊詐騙手法
  - 電子支付詐騙手法
- 帳號密碼的新風險：
  - 多因子認證 (MFA)
  - 無密碼身分識別 (FIDO)
  - 深偽技術 (Deepfake)
- 常見資安事件宣導：
  - 物聯網(IoT)與監視攝影機
  - 郵件社交工程
- 資安法規摘要：
  - 個人資料保護法(個資法)

教學影片 (按訂閱)

智慧時代新生活 YouTube 頻道：
youtube.com/OpenBlueSmartLife

智慧時代新生活 FB 粉絲頁：
facebook.com/SmartEraNewLife