投資人園地

證券投資人及期貨交易人保護中心

問　題	答　覆　內　容
一、吳小姐平常有閒錢就投入股市作為理財方式之一，並以網路、APP 為主要下單方式。她日前於新聞上看到投資人證券帳戶遭惡意駭客的攻擊盜用而下單交易造成損害之情形，不免聯想到自己也是以電子下單為主，所以想瞭解應如何注意以防止個人資料外洩之相關風險？	網路下單快速又便利，目前已為投資人主要下單方式。在享受其便利性之同時，為防止權益受損，投資人宜妥善保管帳號密碼及相關電子憑證，切勿隨意交給他人，以免帳號遭冒用下單；又隨著科技日新月異，投資人除了妥善保管前揭資料外，亦建議留意資安事件的資訊，採行相關因應作為，以維護個人資訊之安全。 近期發生投資人證券交易帳戶遭駭客入侵後以網路下單的資安事件，即駭客利用網路、APP 上民眾外洩的帳號、密碼，在其他網站或平台進行比對，只要比對成功，便可以竊取使用者在該平台的資料。 這是由於很多人為了方便記憶，在不同網站、系統都喜歡使用同一組帳號和密碼，而駭客便是利用投資人這一習慣，用收購或其他方式及管道取得的帳號和密碼，於金融業者網路交易系統進行登錄測試，一旦登錄成功即實際進行交易，而造成投資人之損失。此類資安案事件之發生，即是因使用者過於輕忽或沒注意而使帳號、密碼洩露而使駭客有可乘之機。而關於密碼該如何設定及保管才能有效防止個人資料外洩風險，以下有幾個小撇步可提供予投資人參考： 一、勿使用簡單字元組合或與個資相關密碼（如：12345、出生年月日、身分證字號或電話），儘量使用英文字母及數字的組合來設定密碼，此外，也應定期更改密碼。

中華民國一一一年一月十六日出版

問　題	答　覆　內　容
	二、不要為了方便，把自己的所有網路服務都設定成同樣的帳號與密碼，且應避免一個密碼多用，以減低被盜用的風險。 三、使用網路服務時，不要將密碼及登入資料儲存在電腦中，於使用完畢時，應按「登出」離開網頁並將視窗關閉。另在公共設備上登錄個人帳號時，切記不要勾選「記住帳號密碼」等選項，並應儘可能選擇以匿名方式登錄。 四、使用自動櫃員機（ATM）、或透過電話、網路或在商店購物時提供個人資料或密碼，請注意四周是否有可疑人士，以防止個人資料被竊取。 五、避免使用圖書館、網咖、機場等地之公用電腦從事交易及輸入敏感性高的資訊。 六、儘量記住密碼及個人資料，而不要寫在提款卡、存摺或記事本上，更不要將密碼與存摺、卡片等置放於同一處，避免因未收妥疏忽而被竊取或窺視，導致個人資料外洩。 七、隨時提高警覺防範詐騙集團套取帳號密碼資料並注意新型詐騙手法。 再次提醒投資人應注意密碼的安全性，並確實提高網路安全防範意識，防止帳號密碼被盜，以降低被惡意駭客攻擊的機率而造成嚴重後果！
二、張老先生幾年前從職場退休了，平常最喜歡就是跟老朋友聚會、聊天。在最近的一次聚會中，他聽到朋友說因為接獲網路訊息而加入投資群組，為了獲取高報酬而投入了大筆退休金卻血本無歸，事後才	近期投資詐騙已成為詐騙事件的主要類型之一，部分的受害者是因為不了解歹徒的詐騙手法而受騙造成金錢上的損失；為了保障自身財物的安全，建議投資人平時多留意詐騙事件之相關報導，以及關注相關單位的防詐騙宣導內容，以掌握可能遭遇的詐騙手法，隨時提高警覺並瞭解遭遇詐騙事件的處理方式，以避免受騙而蒙受損失。 以下就目前常見的詐騙訊息傳播管道、態樣，以及發現疑似詐騙事件之處理方式說明如下： 一、常見之詐騙訊息傳播管道： 目前最常見的詐騙管道除電話詐騙及手機簡訊詐騙外，隨著網路科技的便利性提高，通訊軟體 (如 LINE 等)、社群媒體 (如 FB 等)、網路討論區等亦為詐騙資訊傳播的主要管道。 二、詐騙集團常見假冒身分類型：

問　題	答　覆　內　容
發現是遇到了投資詐騙。張老先生想了解目前常見之詐騙態樣有哪些，及應如何提高防騙意識以避免受騙以維護自身權益？	詐騙集團往往假冒特定身分以博取民眾信任，較常聽到的包括假冒檢察官或書記官、警察或調查官、法院人員、電信公司、網購業者，甚至還有假冒 165 反詐騙專線之情形。若屬投資詐騙則常見假冒合法金融業者及其業務人員，或假冒知名人士及投資專家、達人等。 三、各類詐騙訊息傳播管道之注意事項： （一）手機來電： 詐騙集團有竄改來電顯示號碼的技術，常透過顯示為銀行代表號或權威機構電話號碼，向民眾要求帳戶操作或搜集敏感資訊，以誘騙民眾上當。因此，針對電話開頭「+」、來電顯示為「未顯示號碼」或「002」、「009」之來電，務必提高警覺。 （二）手機簡訊： 詐騙集團常用手機簡訊的方式進行詐騙，目前最常見的為網銀簡訊、假冒金融業者及紓困等類型，訊息內容如「銀行帳戶異常」、「介紹飆股」、「通知領取紓困金」等等，通常簡訊中均會夾帶釣魚連結網址或邀請加 LINE 朋友或加入 LINE 群組之連結，以誘導受害者點擊連結或加入好友。 若收到前揭簡訊，切勿點選所附網址，以避免下載惡意程式與帳號密碼被盜取的風險，另亦不要隨意加入簡訊中附有 LINE 群組之投資連結，以免投資不成，反而落入詐騙陷阱。 （三）社群軟體： 近來詐騙集團亦常利用 LINE、FACEBOOK、INSTAGRAM 等通訊軟體邀請投資人加入聊天群、股票交流群等，或利用交友平台網站接觸國內投資人，再藉由社群軟體狩獵肥羊，引導其投資海內外飆股、未上市公司、虛擬貨幣等而蒙受損害。 若收到有疑慮的推薦投資訊息，最好不要理會，更勿貿然加入不明網路群組及輕信網友來路不

問　題	答　覆　內　容
	明之投資管道，以免投資不成反受其害。 四、發現疑似詐騙事件之處理 由於投資詐騙手法日新月異，投資人平常可多留意相關網站訊息以了解最新的詐騙案例與手法；若真的遇到疑似詐騙情況或已實際發生損生，可以電話撥打警政署 165 反詐騙專線進一步求證、報案，或向法務部調查局檢舉；另外，若接收的證券期貨訊息有詐騙疑慮時，亦可撥打證券周邊單位共同設置之證券期貨反詐騙諮詢專線（02）2737-3434 諮詢或查詢訊息來源是否為合法業者，以維護自身權益。

投資人應注意帳號密碼的安全性，並確實提高網路安全防範意識，防止帳號密碼被盜，以避免被惡意駭客攻擊而造成嚴重後果！