關於網路交易安全

（公告事項文件）

公告日期：2019 年 5 月 10 日

關於網站交易安全

滙豐中華證券投資信託股份有限公司（以下簡稱「本公司」）與外界網路連接之網點，設立防火牆控管外界與內部網路之資料傳輸及資源存取，並執行嚴謹的身分辨識作業。因此，機密性及敏感性的資料或文件，不會存放在對外開放的資訊系統中，機密性文件也不以電子郵件傳送，而須讓客戶自行登入查詢。另外，本公司也會定期對內部網路資訊安全設施與防毒進行查核，並更新防毒系統之病毒碼，以及各項安全措施。

辨識詐騙網站與郵件

但是，隨著網路使用人口的增加，頻繁的網路交易讓許多不肖份子認為有機可乘，並不斷以新技術進行網路詐騙。所以，辨識詐騙網站與郵件，也是甚為重要。郵件網路詐騙的主要目的在竊取您的身分資訊，而詐騙者會試圖以欺詐手段獲取您的信任，以取得您的個人資料，例如：銀行帳號、使用者代號、密碼或其他資訊。網路詐騙者的慣常手法是透過大量寄發詐騙郵件以騙取您的個人資料，詐騙郵件的內容通常會提供一個看起來合法又正當的連結網址並要求您點選，一旦您點選了網址，便會被引導到一個偽造的網站，然後詐騙者會要求您提供、更新或確認機密的個人資料。由於詐騙郵件或網站並沒有固定的詐騙模式，所以較難有可依循的辨識準則，如果您看到類似：「請您務必於立即回覆，否則您的帳戶將關閉。」、「如果您不在 12 小時內回應，您的基金款項將無法匯出。」等等的詐騙內容或符號時，請您務必提高警覺，以避免受騙上當。因為，詐騙郵件通常會出現強迫語氣或緊急字眼，也通常會提供一個連結網址或是附有網站上常見的表單供您填寫。詐騙者會要求您點選該連結，由於連結網址會帶有合法公司的名稱以取得您的信任，在不疑有他的情況下，您很可能直接點選，而連結實際上不會連至該網址，而會將您引導至一個偽造的網站，在假網頁上，詐騙者會進一步要求您輸入、確認或更新個人機密資料。由於偽造網站比較難以辨識，為確保您連結至正確的網站，請直接鍵入該網站之網址，例如：您要到本公司官方網站，請直接鍵入 www.assetmanagement.hsbc.com.tw/zh-tw 網址是最安全的方式。一旦您發現有不肖分子假藉本公司名義行詐騙之事，或是收到可疑的電子郵件時，為保護自己以及避免更多人受騙，請您務必來電：0800-007-888 通報詐騙事件，本公司將儘速為您處理。

使用者資訊自我保護

為能有效保護您的資訊安全，也建議您：

（1） 妥善保管您的密碼及或任何個人資料，不要將任何個人資料，尤其是帳號、密碼提供給任何第三人或其它機構。

（2） 每次連線完畢後，務必記得登出會員專區，若您是與他人共享電腦或使用公共電腦，切記要關閉瀏覽器視窗，以防止他人讀取您的個人資料。

（3） 若發現您的密碼或帳號遭到盜用或發生其他安全問題時，應立即通知本公司。