



電子交易安全須知

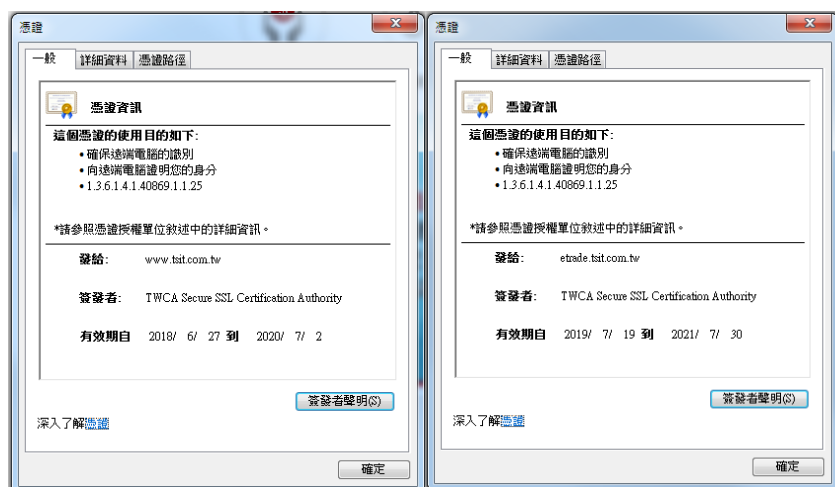
一、妥善保管個人密碼及個人資料

客戶有責任採取合理措施，確保您所使用的密碼安全且保密。在設定密碼時，敬請您特別注意下列各點：

- 請勿於不同的網路銀行使用同一組密碼。
- 請勿使用懶人密碼。
切勿選用容易被猜中的密碼，例如連續或相同的數字或英文字如 12345678、11111111、ABCDEF GH。
- 請勿使用與您個人資料相關的密碼。
例如您的名字、出生日期、電話號碼等。
- 請勿寫下密碼。
我們的建議是使用者代號或密碼應牢記腦中，無論任何時刻，您都不應用筆寫下或用其他方式記下密碼。但如果您需要記下密碼，請確保用來寫下 / 記下密碼的方法不會讓他人輕易取得或推斷到密碼。
- 請定期變更密碼。
請經常不定時變更密碼，且避免重複使用已用過之密碼。
- 請務必將一般網站的密碼，與網路交易的密碼特別區分。
一般網站的密碼可能為明碼，較容易被人猜中或盜用，需特別注意。
- 請勿向任何人透露密碼，包括銀行職員及警方。
- 切勿在公共場所（如網咖或圖書館）使用網路銀行服務，因為這些地方的電腦極有可能安裝了駭客程式，因而使您的密碼外洩。

二、安全憑證

您可藉由瀏覽器網址列的鎖頭標誌「 <https://www.tsit.com.tw>」、「 <https://etrade.tsit.com.tw>」查閱基金電子交易網站的數碼證書有關資料，來辨識是否為正確網站(如下圖所示，最新憑證資訊請以網站為主)。



三、關於防範偽造網站

請注意本公司網站之官網網址為 <https://www.tsit.com.tw/>，電子交易平台網址為 <https://etrade.tsit.com.tw/>，務必確認您是連上本公司的正式網站。

- 每次進入系統應在瀏覽器上輸入網址或將真正的網站記錄在瀏覽器的「我的最愛」中，藉由此兩種管道連結到本公司網站的入口。
- 除非您已完全確定登入本公司網站，否則不應提供任何有關您的交易帳戶的資料。
- 您應對其他網上詐騙活動經常保持高度警覺，以免受騙，招致無謂損失。

四、電腦的保安措施

您應確保您的個人電腦是安全的，並採用適當措施保護電腦，您可採用的措施如下：

- 請定期執行使用者電腦之安全套件更新及增修版程式。一些常用的電腦軟體時常都會發現安全漏洞，一旦發現這種情況，軟體出版商便會推出「增修版程式」供用戶使用來防堵這些漏洞，如用戶電腦未安裝增修版程式，病毒和駭客便可利用此安全漏洞進入這些電腦，盜取資料。
- 請為您的電腦安裝病毒偵測軟體，並定期更新版本、安裝最新的病毒定義檔，以有效保障電腦免受病毒侵襲。
- 請注意，病毒、特洛伊軟件及駭客程式可透過電子郵件傳播，蠕蟲病毒更可將病毒複製及發送至電郵地址簿上各收件人。因此，閣下不應開啟並即時刪除來歷不明的電子郵件，亦不要透過電子郵件提供的超連結登入電子交易服務。
如需開啟電子郵件內的附件，亦應先進行病毒掃描。另外，騙徒亦會藉電郵進行不法活動。
- 請安裝個人防火牆，防火牆是一種小程序，有助於保護您的電腦系統不會在連接網際網路時受到入侵，或所載內容被人擅自盜用。安裝了防火牆，即可阻止資料在未經您授權下上傳或自您的電腦下載。

五、行動裝置的保安措施

您應確保您的行動裝置是安全的，並採用適當措施保護行動裝置，您可採用的措施如下：

- 設定行動裝置時：
 - ◆ 如沒有必要使用基於位置為本的應用程式，應關掉行動裝置內的定位服務設定。
 - ◆ 不應破解行動裝置以解除其使用或存取限制。
 - ◆ Android 使用者請提防 Certifi-Gate 及 Stagefright 漏洞。
- 使用行動裝置時：
 - ◆ 應盡可能使用嚴謹的認證方式，例如雙重認證，保護用於處理敏感資料的網上帳戶。想了解更多有關帳戶保安的提示，你可以瀏覽處理帳戶及密碼指引。
 - ◆ 應小心看守你的行動裝置，一時疏忽都有被竊的可能。
 - ◆ 不應在行動裝置上處理敏感資料，除非使用具有加密功能的或安全的端到端連接。
 - ◆ 不應下載或接受不明或不可靠的程式或內容。
 - ◆ 連接公共的 Wi-Fi 熱點時要謹慎。應避免存取敏感資料，除非採取了足夠的保安措施。
- 備份行動裝置內的資料時：
 - ◆ 將資料同步至雲端服務前應評估保安風險，並採取適當的保安措施，例如避免將敏感資料自動備份或同步至雲端平台上。
 - ◆ 應在許可的情況下，開啟備份/同步軟件之加密選項。
 - ◆ 應確保儲存在桌面電腦或抽取式媒體上的備份都經過加密。
- 棄置行動裝置時：

應確保行動裝置內的數據和設定在棄置前已被完全地刪除。

■ 任何時候：

- ◆ 應把行動裝置放置在安全的地方，尤其是在不使用時。
- ◆ 應時刻留意與行動裝置有關的保安漏洞，並安裝最新的修補程式。
- ◆ 不應在行動裝置上安裝非法或未經授權的軟件。
- ◆ 不應接受不明或不可靠的無線連接要求。

■ 用流動應用程式的注意事項：

- ◆ 只安裝來自官方或可靠來源的流動應用程式。
- ◆ 應安裝流動保安程式(如防禦惡意軟件)，以保護裝置和資料的安全。
- ◆ 應閱讀其他用戶的評語，了解應用程式的使用條款及私隱政策等等。
- ◆ 在安裝或使用流動應用程式時，應徹底審視應用程式的所有權限要求，特別是一些涉及特權的存取。
- ◆ 在許可的情況下，應啟用由流動應用程式所提供保安功能(如密碼保護，安全連接等)。
- ◆ 經常更新系統及流動應用程式至最新版本。
- ◆ 不要下載來歷不明的文件，或打開或點擊可疑或不可靠的連結。
- ◆ 在使用即時通訊應用程式(例如 Whatsapp、LINE、WeChat 等)時，如收到任何詐騙消息後，不應再次轉寄，以免此類詐騙消息進一步散播。
- ◆ 定期檢查已安裝的流動應用程式，並移除一些不再需要的應用程式。
- ◆ 不可移除裝置上設定的使用和存取限制(例如 jailbreak)。
- ◆ 關掉行動裝置內的無線服務例如 Wi-Fi、藍芽(Bluetooth)、近場通訊(NFC)等的自動連線功能。

六、其他安全注意事項

- 本公司不會以電子郵件或電話要求客戶提供私人帳號或密碼，亦不會發送嵌入超連結(包括以 QR 碼形式顯示)、交易網站的電子郵件給您。此外，請勿以電子郵件內的超連結網址進入本公司網站。若發現可疑的電子郵件，請立即向本公司查詢，切勿逕行連結來路不明之網站及鍵入帳號與密碼，或是透過網際網路搜尋引擎或可疑彈出視窗上顯示的超連結存取網站。
- 建議您應嚴格限制任何未經授權的人使用您的電腦，且應避免在使用交易網站服務中途離開電腦。使用完畢應立即登出交易網站服務系統。
- 應時常檢查帳戶餘額及對帳單，或系統操作記錄，以發現是否有異常交易。如發現任何錯漏、未經授權的交易、可疑的登入紀錄、異常的交易網站畫面或彈出畫面等情況，請立即通知本公司。

七、如有任何懷疑，請立即通知下列機構

- 台新投信客服專線：02-2501-3838、0800-021-666
- 反詐騙專線：165