

網上交易服務的安全提示

尊貴的客戶：

鑒於科技罪行及網絡攻擊日趨猖獗，為了保障閣下的帳戶安全，我們建議閣下採取以下各項保障網上活動的措施，加強對網上交易的保護：

I. 有關登入密碼

建議設定一個混合至少 8 個或以上字母及數字的強密碼 (包含大小寫不一的字母、數字及特殊字符混合組成)。並且應定期(最少每六十天)更改密碼，及避免重覆使用同一密碼。

不要將密碼記錄在電腦、手機、或電子設備，以及不要為閣下的不同戶口設定同一密碼: 例如電郵及股票交易帳戶，保護閣下的電腦、手機、或電子設備，閣下可啟動自動上鎖功能。

切勿向任何人透露閣下的登入號碼及密碼〔包括滙業員工、客戶經理、經紀或本公司客戶服務部〕，或回應任何未經核證請求。如有疑問，請聯絡閣下的客戶經理、經紀或本公司客戶服務部。

II. 使用電腦、手機或電子設備

使用可信及安全的電腦、手機或電子設備進行網上交易。完成交易後，即時登出網站或交易系統。避免使用公用電腦或公共無線網絡登入，以及來歷不明或不安全的網絡連接：例如公共無線網絡，進入閣下的網上戶口。

閣下應取消瀏覽器的“自動完成”功能，以避免當閣下鍵入密碼時，電腦會自動完成閣下的輸入。要啟動或取消“自動完成”功能，請打開瀏覽器，選擇“工具” - “Internet 選項” - “內容” - “自動完成設置”，取消“表單上的使用者名稱和密碼”功能。

III. 滙業證券網址及應用程式

可鍵入網址 (滙業證券網址 www.delta-asia.com) 或使用網站書籤，進入滙業網上交易平台，或滙業交易平台(下載版)程式及滙業流動應用程式 (iOS 或 Android 手機版) 登入。切勿透過電郵的超連結、互聯網搜尋器及可疑的彈出視窗登入網站。

IV. 登入過程

當閣下在登入時，請確定沒有人在背後或附近察看，與及確定其他人不能透過手機螢幕看見所輸入的登入名及密碼。

注意任何假冒網站（挪用本公司網站的內容和圖像），可能意圖進行欺詐活動或網路犯罪。當出現不尋常的彈出畫面或視窗、電腦反應異常緩慢，或者一些不尋常的步驟或登入資料的要求時，不要登入閣下的網上戶口，並立即通知閣下的客戶經理、經紀或本公司客戶服務部。

V. 查閱帳戶交易記錄及留意個人資料

仔細查閱網上戶口的所有交易記錄及結餘。定時或在收到經紀的電子提示後，登入閣下的網上戶口，及時查閱戶口所有的交易及戶口結單。如發現任何問題或未經授權之交易應立即通知閣下的客戶經理、經紀或本公司客戶服務部。

請謹防任何未經授權的更改閣下的戶口資料，例如手提電話號碼、電郵地址及登入密碼等。

VI. 安全系統及程式

使用最新版本的操作系統、手機交易應用程式 App、軟件及瀏覽器，確保軟件已及時更新。切勿用 1.)Jailbreak (越獄)¹ 或 2.)Root²機等手法改裝手機及平板電腦。

VII. 提防電腦病毒

切勿下載或開啟可疑的檔案、瀏覽可疑網站或開啟可疑電郵 / 手機短訊的二維碼、超連結及任何附件。

採用可靠的防病毒、防間諜及防惡意攻擊的保安軟件，並在軟件推出新版本時作出更新，以及設定個人的防火牆。

為電腦和手機安裝任何軟件及應用程式前，應考慮數據安全性及私隱的問題。只從官方應用程式商店、程式市場或可信的來源下載及升級應用程式。

VIII. 網絡功能

選用加密的 Wi-Fi 網絡，並移除不必要的 Wi-Fi 連線設定。避免於公共電腦或公共 WiFi 使用滙業交易平台服務。切勿在供公眾使用或連接上未知且不安全的網路的電腦執行任進行任何交易。為減低風險，建議登入閣下的網上戶口時關閉移動裝置上的無線支付功能，如支付應用程式及 NFC 功能等。

¹ 越獄是取得 iOS 裝置的 Root 權限的技術手段。由於獲得了 Root 權限，在越獄之前無法檢視的 iOS 的檔案系統也可檢視。

² Root 通常是針對 Android 系統的手機而言，它使得用戶可以獲取 Android 操作系統的超級用戶權限。