創興商品期貨
Chong Hing Commodities & Futures
(創興銀行全資附屬機構)
(A Wholly-Owned Subsidiary of Chong Hing Bank)

客戶通告
網絡保安警惕及預防未經授權的期貨合約交易

為保障 閣下的期貨投資安全，防範未經授權的期貨合約交易及網絡詐騙，客戶請務必留意以下事項並採取預防措施，避免招致財務損失。

- 妥善保管賬戶資料，切勿向他人或透過未經核實的網站透露您的期貨合約交易賬號、網上交易平台之登入名稱和密碼、一次性驗證碼 (OTP）或個人身份資料等，避免使用公共電腦或未加密的 Wi-Fi 網絡登入交易賬戶。
- 定期查核與賬戶有關的任何異常活動，例如查閱獲發送的有關系統登入、密碼重置、交易執行或客戶和賬戶相關資料變更的通知，以識別攻擊者試圖進行未經授權的期貨合約交易（不論成功與否）的跡象。
- 不要輕信任何電子郵件，對於任何要求您提供個人信息的電子郵件保持高度警惕。習慣檢查發件人的電子郵件地址，並避免點擊可疑鏈接。
- 啟用雙重驗證功能，以增加額外的安全層級。這樣即使密碼被盜取，未經授權的訪問仍會受到限制。
- 加強密碼安全， 使用高強度密碼（結合英文大小寫、數字及符號），並定期更換，避免使用容易猜到的個人信息及在多個平台重複使用同一密碼。
- 接收電子郵件或短訊必須保持警覺，不應點擊任何內含的超連結。如不慎點擊內含的超連結，及因而被引導至任何網站或流動應用程式的話，切勿輸入任何敏感或機密的個人資料，例如用作登入賬戶所需的用戶資料及一次性密碼等。
- 適時就其個人資料 (例如：簽署式樣、通訊地址、手機號碼及電郵地址等) 的任何變更通知本公司。
- 經常保持操作期貨合約交易的電子設備安全，確保您的電腦和移動設備安裝有最新的防病毒軟件和安全更新，以防止惡意軟件的攻擊。
- 定期檢查您的期貨合約交易記錄和賬戶餘額，盡快核對相關交易文件（包括期貨賬戶成交結單），並在期貨賬戶出現任何差異或懷疑（或確定）期貨賬戶曾發生未經授權交易時，應儘速向本公司客戶服務處職員（而非操作期貨合約交易的客戶主任）(熱線：3768 9988) 作出跟進。
- 亦可就未經授權的期貨合約交易事故保留相關證據（如通話記錄、電郵或截圖）立即向香港警務處（警方）舉報。

創興商品期貨
Chong Hing Commodities & Futures
(創興銀行全資附屬機構)
(A Wholly-Owned Subsidiary of Chong Hing Bank)

常見投資詐騙手法

- 提防假冒金融機構或投資顧問，詐騙者可能冒充公司職員、監管機構或「投資專家」，透過電話、電郵或社交媒體誘騙您提供賬戶資料或轉賬。切勿輕信「高回報、零風險」的投資建議。

- 提防偽造網站，檢查網站網址是否正確（如 HTTPS 加密及官方域名），防範釣魚網站。務必確認訪問的網站網址正確無誤，特別是在登錄您的賬戶之前。仿冒網站常常使用類似的網址來欺騙用戶。

- 提防偽造網站及假冒應用程式，僅透過官方網站或應用商店下載手機應用程式，避免點擊來歷不明的連結，正規持牌法團不會要求客戶透過不明連結登入或轉賬至個人賬戶。

- 提防社交工程詐騙，不要在社交媒體或公共平台上分享您的財務信息或個人識別信息，時刻警惕聲稱「中獎」、「賬戶異常」或「緊急操作」的來電或訊息，詐騙者常製造恐慌以誘導您洩露資料。如有疑問，請直接聯絡本公司客戶服務熱線 3768 9988。

“防騙視伏器”和流動應用程式“防騙視伏 App”

- 使用“防騙視伏器”和流動應用程式“防騙視伏 App”，用戶可在“防騙視伏器”的數據庫中進行搜索，以查核某網站、電話號碼、電郵等是否可能涉及欺詐。有關“防騙視伏 App”如偵測到用戶嘗試瀏覽可能涉及欺詐的網站，更可實時向用戶發出警示。詳情請瀏覽下列「守網者」網站。

關於網絡保安威脅及詐騙的訊息，請瀏覽以下網站

- ✧ **守網者** https://cyberdefender.hk/
- ✧ **反詐騙協調中心** https://www.adcc.gov.hk/zh-hk/home.html
- ✧ **投資者及理財教育委員會** https://www.ifec.org.hk/web/tc/index.page
- ✧ **證監會的警示名單** https://www.sfc.hk/TC/alert-list

09/2025