

親愛的客戶：

貴金屬及外匯孖展服務實施雙重認證

本行致力提供安全穩妥的網上和流動電話銀行服務，為讓閣下使用時得到更佳保障，由 2024 年 11 月 15 日起，透過網上銀行/流動電話銀行進入貴金屬及外匯孖展交易平台，將需使用流動保安編碼或保安編碼器進行雙重認證。

閣下可透過 App Store、Google Play 或本行網站下載「交通銀行(香港)手機銀行」流動應用程式以啟動流動保安編碼。

重要訊息

數碼 KEY 睇緊啲 撇 LINK 前要三思

網上銀行的個人登入資料(包括賬戶名稱、登入密碼和一次性密碼)在互聯網世界中就如家裏門匙一樣重要，必須妥善保管。

按金管局的監管要求，本行不會透過短訊或電郵發送超連結，引領客戶到本行網站或流動應用程式進行交易，更不會透過超連結要求客戶提供任何敏感的個人資料(包括登入密碼和一次性密碼)。

如果客戶收到任何短訊或電郵所發送的超連結，要求輸入網上銀行個人登入資料，這些短訊或電郵不應是由本行發出的。客戶在點擊任何聲稱為銀行發出的超連結之前，應「三思而後行」，如有疑問應立即聯絡本行查詢。

謹慎處理手機應用程式

請格外警惕能夠操控您的手機的惡意軟件。當您被邀請打開可疑連結或下載應用程式，請三思而後行，在安裝前應先仔細評估相關手機應用程式的權限需求，如果發現可疑的權限需求，切勿安裝相關手機應用程式。除非完全確定，切勿允許系統安裝來歷不明手機應用程式。

重要保安提示

1. 請勿設定單一私人密碼以登入不同網上服務，網上銀行/流動電話銀行密碼不應與其他服務共用。
2. 每次登入網上銀行/流動電話銀行服務時，請檢查上一次的登入紀錄，如發現可疑登入情況，應立即致電客戶服務熱線 223 95559 與客戶服務員聯絡。
3. 如登入過程中有異樣(如出現不尋常的視窗彈出或被要求提供額外的個人資料等)，應立即停止登入並登出網上銀行/流動電話銀行並致電客戶服務熱線 223 95559 通知本行。
4. 切勿向任何第三方服務提供者披露您的用戶名稱、密碼及一次性密碼，不論其是否已獲本行授權。
5. 使用網上銀行或流動電話銀行服務時應在瀏覽器直接輸入「交通銀行(香港)」網站(www.hk.bankcomm.com)或透過 App Store、Google Play 或交通銀行(香港)網站下載及安裝交通銀行(香港)流動應用程式接駁至網上銀行或流動電話銀行賬戶，切勿下載或安裝來源不明的軟件及應用程式。

6. 若客戶曾透過第三方網站、第三方流動應用程式等登入交通銀行(香港)網上銀行或流動電話銀行，本行建議客戶盡快更改密碼，以保障個人資料安全。客戶如發現其賬戶有任何未經授權交易，或對網上銀行、流動應用程式有任何疑問，請致電客戶服務熱線 223 95559 查詢。
7. 採用本行建議使用的 iOS/Android 操作系統使用流動電話銀行服務/證券流動應用程式，本行現時建議使用之操作系統：

流動電話銀行服務	證券流動應用程式
iOS 13.0 或以上 iPhone Android 8.0 或以上手機	iOS 12.0 或以上 iPhone Android 8.0 或以上手機

8. 建議閣下將流動電話銀行服務/證券流動應用程式升級至最新版本。
9. 為協助客戶對欺詐、詐騙和欺騙活動保持警惕，本行根據從香港警務署的「防騙視伏器」不時接收到的風險警告、訊息及指標發出風險警示。
- (i) 當閣下輸入「轉數快」收款識別代號(手機號碼/電郵/快速支付系統識別碼)進行「轉數快」轉賬時，若「轉數快」識別代號與「防騙視伏器」內的「高危有伏」標籤吻合，於確認交易前會向客戶發警示，要求閣下核實是否繼續交易。請留意上述情況，並按警示停止交易(如適用)及留意相關交易為高風險交易，若客戶繼續交易需承擔相關風險。
- (ii) 閣下可於轉賬前善用警方「防騙視伏器」作即時評估詐騙及網絡安全風險。
- (iii) 若有任何懷疑，可致電警方反詐騙協調中心的「防騙易 18222」熱線尋求協助或向警方舉報。
10. 請格外警惕能夠操控您的手機的惡意軟件。當您被邀請打開可疑連結或下載應用程式，請三思而後行，在安裝前應先仔細評估相關手機應用程式的權限需求，如果發現可疑的權限需求，切勿安裝相關手機應用程式。除非完全確定，切勿允許系統安裝來歷不明手機應用程式。
11. 本行會定期檢討此保安提示以確保其足夠及合適，請閣下不時查閱本行提供的保安建議。

有關更多網上銀行或流動電話銀行之保安資訊，請瀏覽本行網頁之保安資訊或流動電話銀行 (生活 > 服務及資訊 > 更多 > 重要提示) 內之保安提示。

如您對本函內容有任何查詢，請致電客戶服務熱線 223 95559 與本行客戶服務員聯絡。

交通銀行(香港)有限公司(於香港註冊成立的有限公司)謹啟

(本函為無需簽署之電腦簽印文件)