客戶通知 – 小心電子網絡詐騙

近日香港的電子網絡騙案有上升趨勢，東亞證券有限公司（「東亞證券」或「本公司」）謹此提醒客戶，在收到任何聲稱代表東亞證券發出的電郵和任何即時電子訊息時（如手機短訊、WhatsApp、微信等），請時刻保持警覺。另外，亦請客戶留意以下的提示，慎防受騙：

- 東亞證券不會透過電郵或即時電子訊息，要求客戶透露香港身份證號碼、賬戶號碼、登入密碼、或一次性密碼等任何敏感資料。

- 請小心提防任何聲稱代表本公司，但發出自非正式的渠道，例如一些與本公司官方電郵地址相似的電郵地址。

- 東亞證券不會要求客戶跟從或按下任何超連結以進行交易。

若客戶對任何收到的信息有懷疑，請立即致電本公司客戶服務熱線 (星期一至五早上 9 時至下午 5 時（852）3608 8021) 或親臨香港德輔道中 10 號東亞銀行大廈 9 樓與我們聯絡。另外，您亦可以聯絡香港警務處反詐騙協調中心（Anti-Deception Coordination Centre）：（852）18222，諮詢有關反詐騙事宜。

關於更多保安提示，請閱讀以下資訊。

保安提示

為確保您的交易及個人資料安全，建議您先閱讀以下資訊。

1. 保安提示要點
2. 使用東亞證券電子網絡股票買賣服務系統（包括互聯網及手機應用程式）
3. 使用自動化電話服務
4. 雙重認證
5. 防止詐騙資訊
6. 更多保安資訊

1. 保安提示要點

- 切勿向其他人透露您的東亞證券電子網絡股票買賣服務系統（包括互聯網及手機應用程式）的使用者號碼、密碼或一次性密碼。
- 切勿打開可疑的電子郵件附件，或點擊附於任何電子郵件、短訊、即時通訊訊息、社交媒體平台、二維碼、搜索引擎或不可靠來源內的超連結並進入網頁及輸入敏感資料 – 特別是您的登入資料。如需使用網上服務，應直接於瀏覽器輸入 www.easecurities.com.hk 網址、把網址設為書籤或使用東亞證券電子網絡股票買賣服務 - 手機應用程式。
- 如您遇到可疑來電、網購賣家、交友邀請、招聘廣告、投資網站等，建議您在進行交易前可點擊「防騙視伏器」https://cyberdefender.hk 查詢相關平台賬戶名稱、收款賬戶、電話號碼、電郵地址、網址等，以評估詐騙及網絡安全風險。
- 慎防網絡釣魚詐騙（例如假冒來自政府或金融機構為主題的網絡釣魚詐騙等）、駭客、病毒、間諜軟件及其他惡意程式入侵。
- 及時留意本公司發出的短訊/電郵交易提示，並定期透過東亞證券電子網絡股票買賣服務系統(包括互聯網及手機應用程式）查閱賬戶交易及結單。若發現可疑情況，應立即通知本公司。
- 使用官方軟件並確保您裝置上的作業系統及應用程式已裝有最新的安全更新，不時更新防毒軟件和防間諜軟件並定期掃瞄您的裝置。
- 請設定一個難以猜破的密碼，密碼要求為至少八個字元，避免使用容易讓人取得的個人資料，如電話號碼或出生日期作為密碼。該密碼應與其他網上服務之密碼不同，並定期更改密碼。
- 切勿在不同網上或社交媒體的賬戶使用相同的密碼。如您懷疑有人得知您的密碼，建議您立即更改密碼，如需要可聯繫本公司尋求幫助。

2. 使用東亞證券電子網絡股票買賣服務系統（包括互聯網及手機應用程式）

- 登入時需先留意四周環境，切勿讓他人得知輸入的資料和使用後正確地登出。
- 為確保交易安全，請透過官方應用商店(如: Google Play 或 App Store 應用程式市場)，並切勿在任何已被「越獄破解」或「超級用戶權限破解」的裝置使用。
- 首次使用網上服務時應立即更改您的密碼，然後銷毀載有密碼之文件。
- 每次登入本公司電子網絡股票買賣服務系統（包括互聯網及手機應用程式）時，請留意上次登入的日期及時間或「確認訊息」。
- 如您於本公司登記的流動電話號碼及/或電郵地址已更改或已失效，請即到本公司、東亞銀行任何一間分行或登入東亞證券電子網絡股票買賣服務系統 - 互聯網更新個人資料。
- 為防止他人未經授權使用，本公司建議您為您的裝置設立自動上鎖、啟用密碼鎖及啟動遠端清除等功能。當您的裝置有遺失/被盜的情況，建議您登入東亞證券電子網絡股票買賣服務系統（包括互聯網及手機應用程式）更改您的東亞證券電子網絡股票買賣服務系統密碼（包括互聯網及手機應用程式），並停用您的 i-Token (如適用) 。
- 當發現或懷疑您的賬戶被他人未經授權使用時，請立即通知本公司。
- 請妥善保管用以登入東亞證券電子網絡股票買賣服務系統的電腦及手機。如您的裝置能使用生物認證（如指紋或面容辨識），切勿停用任何有助提升生物認證安全性的功能，並不要讓任何人在您的裝置上登記其生物信息。
- 如您有多胞胎或面容相像的兄弟姊妹，或正處於面部特徵可能快速發展的青春期，請不要使用面部辨識作認證。

- 切勿透過公共電腦或公共/不知名無線網絡登入網上服務。當使用 Wi-Fi 登入網上服務時，應選用加密的網絡，並移除不必要的 Wi-Fi 連線設定。如無須使用請關閉 Wi-Fi、藍芽、NFC 等無線網絡功能。
- 避免透過免費或不可靠的虛擬專用網絡(VPN)使用網上服務。如果需要使用遠程控制技術來使用網上服務，請利用沒有已知漏洞的可靠軟件。
- 細閱網站、應用程式和其他軟件及程式的安裝及/或許可請求。切勿於您的裝置上安裝或運行來自第三方/來歷不明的應用程式，必要時移除任何可疑應用程式。
- 定期檢查並更新您的系統瀏覽器及東亞證券的官方流動應用程式。
- 當使用公共 USB 充電站充電手機或設備時，需留意情況以避免感染惡意軟件。
- 請勿在可疑網站或應用程式提交文件（例如身份證掃描檔案，銀行賬單和信件）。

3. 使用自動化電話服務

- 為防止欺詐行為，請將自動化電話服務密碼保密。
- 切勿將自動化電話服務密碼告知他人(包括本公司職員或警方)。
- 切勿讓他人使用您的自動化電話服務密碼進行查詢/交易。
- 定期更改您的自動化電話服務密碼以確保安全。

4. 雙重認證

- 為提升網上交易安全，本公司已為相關電子渠道提供雙重認證服務。登入時，您需要使用 i-Token*或輸入本公司發出的一次性短訊交易密碼#。
- 請妥善保管您的雙重認證工具。切勿讓您的安全設備（包括已啟動 i-Token 或接收一次性短訊交易密碼的手機）處於無人看管狀態，或讓其他人使用或控制該設備。
- 切勿向任何人透露發送至您手機的一次性密碼。
- 切勿在任何已被「越獄破解」或「超級用戶權限破解」的裝置安裝使用 i-Token。

*客戶必須於本公司登記流動電話號碼及電郵地址後，才可登記及使用 i-Token。

即使您已啟動香港流動電話服務商提供的「短訊轉駁」服務，本公司所發出載有一次性短訊交易密碼的流動短訊亦不會被轉送至其他電話號碼。

5. 防止詐騙資訊

- 若您對任何推廣東亞證券產品或服務之代表的身份有懷疑，應立即透過官方渠道致電本公司與職員核實來源。
- 若您早前在開立戶口時提供給本公司的身份證明文件已遺失及/或隨後已更換，或您懷疑您的個人資料、結單或賬戶資料可能已被洩露或盜取，應立即通知本公司。
- 慎防偽冒短訊及語音訊息來電。如您對來電者有懷疑，應立即透過官方渠道致電本公司與職員核實。
- 慎防有騙徒偽冒為東亞證券的職員行騙。慎防未經授權股票交易。如發現您的賬戶有任何可疑或未經授權的交易，應立即透過官方渠道致電本公司與職員查詢。
- 回應電郵要求前請先經其他渠道核實電郵發放者身份，提防受騙。
- 慎防一些潛在網絡釣魚攻擊的訊號，例如可疑的發件人地址、標題以"警告" 或 "FYI"為題和內容要求您輸入個人資料或按下可疑連結、使用通用稱呼、用威脅或緊迫性的文字、要求提供敏感資料或指示您打開附件而內容包含不清晰的拼寫/語法等，請通過另一 / 官方渠道驗證發件人的身份或立即將其刪除。
- 在輸入一次性短訊交易密碼之前，請確定網站是可信任的。
- 採取預防措施以保護您用以進入東亞證券電子網絡股票買賣服務系統（手機應用程式）的所有手機，並防止其他人使用該手機。
- 為避免您墮入任何網絡詐騙的陷阱，建議您留意香港金融管理局、香港警務處或其他認可機構發出的防騙資料及最新消息。

6. 更多保安資訊

如欲了解更多保安資訊，請按下列連結：

香港警察：

- 預防科技罪案
- 什麼是釣魚攻擊
- 什麼是網上帳戶騎劫?
- 什麼是 WhatsApp 戶口騎劫?

反詐騙協調中心 - 防騙短片/警示：

- 最新騙案警示
- 「A 股」投資詐騙
- 電話詐騙
- 騙案 - 喜怒哀「落」
- 網絡投資騙案
- 「名人效應」投資騙案
- 網上情緣暨投資騙案
- 網上求職騙案
- 網絡釣魚騙案

香港特別行政區政府：

- 網絡安全資訊站
- 資訊安全網

香港金融管理局：

- 數碼 KEY 睇緊啲，撳 LINK 前要三思! - 信用咭篇
- 數碼 KEY 睇緊啲，撳 LINK 前要三思!
- 智醒銀行 客戶錦囊　網上銀行服務
- 智醒銀行 客戶錦囊　櫃員機
- 保護個人數碼鎖匙
- 智醒消費者 小心騙徒
- 係咪呃緊你？Check 吓「防騙視伏器」

如果您發現任何可疑交易或收到可疑交易通知，請立即致電本行客戶服務熱線(星期一至五早上 9 時至下午 5 時（852）3608 8021) 或親臨香港德輔道中 10 號東亞銀行大廈 9 樓與我們聯絡。另外，您也可以聯絡香港警務處反詐騙協調中心（Anti-Deception Coordination Centre）：（852）18222，諮詢有關反詐騙事宜。