

偽冒網站及交易平台聲明

網絡詐騙案件日益猖獗，偽冒網站及交易平台頻現，以及發送欺詐短訊偽冒凱基。凱基特此提醒您慎防偽冒網站、交易平台及未經授權的交易，並重申以下為凱基的官方網站、交易平台、微信帳號及短訊發送人名稱。

凱基官網	<p>https://www.kgi.com.hk/zh-hk/homepage/</p> 
交易平台	<ul style="list-style-type: none">• 凱基投資通• SPTrader Pro HD• 網上投資服務(WebTrade)• 網上投資服務 - 專業版 (WebTrade - Professional Version)• 出期智勝SP/出權智勝
微信帳號	<p> KGI 凱基 KGI HONG KONG LIMITED  中国香港</p> <p>帳號名稱：KGI 凱基 WeChat ID：KGI_HK</p>

<p>短訊發送人名稱 (香港)</p>	<p>凱基已加入短訊發送人登記制，使用已登記發送人名稱包括#KGI_ASIA及#KGI_FUT，向本地流動電話用戶發出單向短訊，以便您識別凱基短訊。</p> <div> <div> <p>• 凱基亞洲將以「#KGI_ASIA」開首</p>  </div> <div> <p>• 凱基期貨將以「#KGI_FUT」開首</p>  </div> </div>
<p>香港及海外電話 用戶短訊</p>	<p>短訊以【KGI】、【KGIA】或【KGIF】為開首，以資識別。</p> <div>   </div>
<p>中國內地電話用 戶短訊</p>	<p>短訊以「【讯格得】凱基:」為開首，以資識別。</p> 

請必須通過凱基的官方網站下載應用程式，並留意以正確應用程式名稱進行搜尋，以免下載假冒應用程式。偽冒網站或提供載有二維碼的下載連結，但這些應用程式均不是凱基的官方應用程式。

凱基絕不會要求您透過超連結提供個人敏感資料，例如登入資訊、一次性密碼。請勿向任何未經核實的網站、應用程式或平台披露帳戶登入資料，即使這些網站看似真實。

在任何情況下，切勿向任何人士披露或容許任何人使用您的密碼，包括凱基的員工。凱基絕對不會以任何方式，如電郵、電話、短訊、即時通訊軟件等，要求您提供密碼及個人敏感資料。

同時您亦應：

- a) 避免點擊短訊內含的超連結，以及避免在偽冒網站或流動應用程式中，輸入機密的個人資料、用戶資料及一次性密碼；
- b) 定期查核與帳戶有關的任何異常活動，例如查閱有關系統登入、密碼重置、交易執行或和帳戶相關資料變更的通知，以識別攻擊者試圖進行未經授權交易的跡象；
- c) 如選擇不接收交易執行通知，便要警惕相關風險，您亦可致電我們的 24 小時專線(852) 2878-5555 或向您的客戶經理重新選擇接收該等通知；
- d) 如懷疑或確定帳戶曾發生未經授權交易，請立即聯絡凱基，電話：(852) 2878-5555；
- e) 就任何未經授權交易事故立即向香港警務處（警方）舉報；
- f) 可使用「防騙視伏器」和流動應用程式「防騙視伏 App」（詳情見 <https://cyberdefender.hk/scameter/>）。例如：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。「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，用戶亦可透過「防騙視伏 App」向警方舉報可疑的網站、電話號碼、電郵地址及仿冒連結，以使詐騙行為可被識別及被載入一個可供公眾查閱的數據庫中。

了解更多網絡安全指引

值得信賴及可靠的資源：

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

凱基在此重申，本集團與這些偽冒網站概無任何關係，並且不會就該網站及其內容或任何與或透過該網站進行的交易承擔任何責任或義務。

凱基在此明確保留所有權利，包括但不限於採取法律行動。

如有查詢，請致電我們的 24 小時「綜合投資專線」(852) 2878-5555 或聯絡您的客戶經理。

凱基證券亞洲有限公司
凱基期貨(香港)有限公司