ICBC 中国工商银行（亚洲）

AI 代理火熱之際 如何做個謹慎投資者

隨着人工智能科技的快速發展，AI 工具逐漸普及，最近火熱的開源人工智能代理被不少投資者作為智能投資助理，為投資操作帶來便利，但其背後潛藏的安全風險同樣不容忽視。騙徒及網絡攻擊者常利用 AI 工具漏洞進行詐騙，用戶若疏忽防範，極易導致賬戶被盜，造成巨額財產損失。為避免成為下一個受害者，保障投資者資金與賬戶安全，本文將提醒各類使用風險，並提供防範要點，助你遠離投資安全隱患。

常見的 AI 代理使用風險

一、授權操作風險

近年來，隨著 AI 辦公應用工具的功能逐漸强大，部分用戶熱衷於將辦公或個人電腦的操作權限全權授權給 AI 代理，放手任程序自動運行任務以實現全自動化辦公。但隨著用戶量快速增多，任務量日益龐大，近期爆出多項 AI 代理超預期地未經許可便刪除用戶重要郵件、或刪除程序內重要代碼、或卸載系統內重要應用的案例，甚至使用客戶的投資賬戶進行交易，造成實際損失。授權 AI 代理的操作風險貌似已不可忽視。

二、密碼洩露風險

投資賬戶授權密碼是賬戶安全的核心屏障，部分用戶為圖方便，設置簡單密碼或重複使用同一密碼，並授權 AI 代理可隨意登陸，在所使用設備未獲得充分防護的情況下，極易導致賬戶密碼、IP 地址等隱私信息被網絡黑客破解盜取，並擅自進行投資交易、轉移資金。用戶往往無法及時察覺，最終損失難以挽回。

三、授權 AI 應用於投資的風險

AI 的投資輔助功能僅為數據分析與參考建議，並非專業投資決策。部分用戶過度依賴 AI 授權操作，全權交由 AI 代理執行投資買賣、資產配置，忽視市場波動與 AI 算法局限：AI 分析基於歷史數據，無法預測未發生的突發市場風險、政策變動；且授權 AI 代理全權操作後，用戶喪失人工監控環節，若 AI 代理出現算法偏差、數據錯誤、或系統崩潰，將直接為投資者帶來損失；且自動化執行交易後，責任主體及相關法律責任定存在較大不確定性風險。

四、非法鏈接與偽冒平台風險

騙徒常偽造 AI 代理官方登錄鏈接、仿冒 APP，以「升級優化」「專屬投資通道」為誘餌，引誘用戶點擊授權、輸入賬戶密碼。用戶一旦在非法渠道登錄，賬戶信息將直接被騙徒獲取。部分偽冒平台還會假借 AI 投資名義，誘導用戶授權高風險交易，騙取投資者資金。

AI 代理安全使用貼士

1. 嚴守授權密碼安全

用戶應設置複雜及具有獨特的密碼、定期進行更換、不與其他平台密碼通用及不授權 AI 代理無限制使用個人密碼、驗證碼，可有效降低密碼被偷盜之風險。另外，在使用 AI 代理前，建議妥善設置好網絡防火牆、防毒軟件等網絡防護措施，不建議在公共網絡、陌生設備登錄賬戶，如有需要登錄，登錄後應及時退出並清除緩存，杜絕密碼被黑客攻擊與洩露風險。

2. 理性對待 AI 投資授權

用戶應明確指示 AI 分析結果僅供投資參考，不應授權 AI 代理全權執行投資交易；亦不應盲從大衆使用 AI 代理，而是在使用前，先充分了解其特性、限制、以及能力，並結合市場行情、自身風險承受能力、以及人工分析核實，避免過度依賴 AI 全自動操作而引發虧損。

3. 核實官方渠道信息

僅通過 AI 代理發行商官方網站、認證應用商店下載登錄平台，不點擊陌生鏈接、安裝不明來源 APP；遇「授權優惠」「AI 穩賺」等可疑信息，第一時間通過官方客服核實，杜絕上當受騙。

4. 提升數據安全意識

定期檢查賬戶交易記錄，及時發現異常交易；用戶應開啟賬戶異常提醒功能。如遇未授權登錄或交易，用戶應即時聯繫官方機構並凍結賬戶；避免招致損失。

5. 杜絕僥倖貪心心理

切勿輕信「AI 投資穩賺高回報」「授權即享收益」等虛假宣傳，所有形式的投資均伴隨著風險，無全自動無風險的投資模式，投資者應保持理性，便宜勿貪。

提示:
數碼 KEY 睇緊啲，撳 LINK 前要三思！
借賣戶口中圈套，助洗黑錢毀前途。
投資涉及風險。

ICBC 中国工商银行（亚洲）

風險披露：
證券交易的風險：投資涉及風險，證券價格有時可能會非常波動，證券價格可升可跌，甚至變成毫無價值。買賣證券未必一定能夠賺取利潤，反而可能會招致損失。

重要聲明
以上風險披露聲明不能披露所有涉及的風險，如欲索取完整之風險披露聲明，可向本行各分行查詢。投資前應先閱讀有關產品發售檔、財務報表及相關的風險聲明，並應就本身的財務狀況及需要、投資目標及經驗，詳細考慮並決定該投資是否切合本身特定的投資需要及承受風險的能力。本行建議您應於進行任何交易或投資前尋求獨立的財務及專業意見，方可作出有關投資決定。本文章所載資料並不構成招攬任何人投資於本文所述之任何產品。本文章由中國工商銀行(亞洲)有限公司刊發，內容未經證券及期貨事務監察委員會審閱。
「本行」或「中國工商銀行（亞洲）」乃中國工商銀行（亞洲）有限公司之簡稱。