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)

客户通告
网络保安警惕及预防未经授权的期货合约交易

为保障 阁下的期货投资安全，防范未经授权的期货合约交易及网络诈骗，客户请务必留意以下事项并采取预防措施，避免招致财务损失。

- 妥善保管账户资料，切勿向他人或透过未经核实的网站透露您的期货合约交易账号、网上交易平台之登入名称和密码、一次性验证码 (OTP）或个人身份资料等，避免使用公共电脑或未加密的 Wi-Fi 网络登入交易账户。
- 定期查核与账户有关的任何异常活动，例如查阅获发送的有关系统登入、密码重置、交易执行或客户和账户相关资料变更的通知，以识别攻击者试图进行未经授权的期货合约交易（不论成功与否）的迹象。
- 不要轻信任何电子邮件，对于任何要求您提供个人信息的电子邮件保持高度警惕。习惯检查发件人的电子邮件地址，并避免点击可疑链接。
- 启用双重验证功能，以增加额外的安全层级。这样即使密码被盗取，未经授权的访问仍会受到限制。
- 加强密码安全， 使用高强度密码（结合英文大小写、数字及符号），并定期更换，避免使用容易猜到的个人信息及在多个平台重复使用同一密码。
- 接收电子邮件或短讯必须保持警觉，不应点击任何内含的超连结。如不慎点击内含的超连结，及因而被引导至任何网站或流动应用程式的话，切勿输入任何敏感或机密的个人资料，例如用作登入账户所需的用户资料及一次性密码等。
- 适时就其个人资料 (例如：签署式样、通讯地址、手机号码及电邮地址等) 的任何变更通知本公司。
- 经常保持操作期货合约交易的电子设备安全，确保您的电脑和移动设备安装有最新的防病毒软件和安全更新，以防止恶意软件的攻击。
- 定期检查您的期货合约交易记录和账户余额，尽快核对相关交易文件（包括期货账户成交结单），并在期货账户出现任何差异或怀疑（或确定）期货账户曾发生未经授权交易时，应尽速向本公司客户服务处职员（而非操作期货合约交易的客户主任）(热线：3768 9988) 作出跟进。
- 亦可就未经授权的期货合约交易事故保留相关证据（如通话记录、电邮或截图）立即向香港警务处（警方）举报。

常见投资诈骗手法

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)

- 提防假冒金融机构或投资顾问，诈骗者可能冒充公司职员、监管机构或「投资专家」，透过电话、电邮或社交媒体诱骗您提供账户资料或转账。切勿轻信「高回报、零风险」的投资建议。

- 提防伪造网站，检查网站网址是否正确（如 HTTPS 加密及官方域名），防范钓鱼网站。务必确认访问的网站网址正确无误，特别是在登录您的账户之前。仿冒网站常常使用类似的网址来欺骗用户。

- 提防伪造网站及假冒应用程式，仅透过官方网站或应用商店下载手机应用程式，避免点击来历不明的连结，正规持牌法团不会要求客户透过不明连结登入或转账至个人账户。

- 提防社交工程诈骗，不要在社交媒体或公共平台上分享您的财务信息或个人识别信息，时刻警惕声称「中奖」、「账户异常」或「紧急操作」的来电或讯息，诈骗者常制造恐慌以诱导您泄露资料。如有疑问，请直接联络本公司客户服务热线 3768 9988。

“防骗视伏器＂和流动应用程式“防骗视伏 App＂

- 使用“防骗视伏器＂和流动应用程式“防骗视伏 App＂，用户可在“防骗视伏器＂的数据库中进行搜索，以查核某网站、电话号码、电邮等是否可能涉及欺诈。有关“防骗视伏 App＂如侦测到用户尝试浏览可能涉及欺诈的网站，更可实时向用户发出警示。详情请浏览下列「守网者」网站。

关于网络保安威胁及诈骗的讯息，请浏览以下网站

- ✧ **守网者** https://cyberdefender.hk/zh-cn/
- ✧ **反诈骗协调中心** https://www.adcc.gov.hk/zh-cn/home.html
- ✧ **投资者及理财教育委员会** https://www.ifec.org.hk/web/sc/index.page
- ✧ **证监会的警示名单** https://sc.sfc.hk/TuniS/www.sfc.hk/TC/alert-list

09/2025