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)

Customer Notice

Internet Security Alert and Precautions Against Unauthorized Futures contract trading

To protect your futures investments and guard against unauthorized futures contracts trading and online fraud, please pay attention to the following points and take preventative measures to avoid financial losses.

- Keep your account information confidential. Do not verify your futures contracts trading account number, online trading platform login name and password, one-time verification code (OTP), or personal information with others or on unauthorized websites. Avoid logging in your trading account using public computers or unencrypted Wi-Fi networks.

- Regularly review any unusual account activity, such as identifying notifications regarding system logins, password resets, trade executions, or changes to customer and account information, to identify any unauthorized futures contract trading attempts (both successful and unsuccessful).

- Do not trust any emails easily. Be extremely cautious of any emails requesting personal information. Regularly check the sender's email address and avoid clicking on suspicious links.

- Enable two-factor authentication for an additional layer of security. This will limit unauthorized access even if the password is stolen.

- Enhance password security by using strong passwords (combining uppercase and lowercase letters, numbers, and symbols) and changing them regularly. Avoid using easily guessed personal information or reusing the same password across multiple platforms.

- Be vigilant when receiving emails or text messages and avoid clicking on any hyperlinks contained within them. If you accidentally click on a hyperlink and are directed to a website or mobile application, do not enter any sensitive or confidential personal information, such as user information and plugin passwords required to log in to your account.

- Notify our company of any changes of the personal information promptly (e.g., signature form, mailing address, mobile phone number, and address).

- Always keep electronic devices used for futures contract trading secure and ensure your computer and mobile device are installed with the latest antivirus software and security updates to prevent malware attacks.

- Regularly review your futures contract trading records and account balances, review and verify the relevant transaction documents (including futures trading account transaction statements) promptly, and report any discrepancies in your futures contract trading account or suspicions (or confirmations) of unauthorized transactions to our Customer Service staff (relationship managers who do not handle futures contract transactions) (hotline: 3768 9988) for follow-up as early as possible.

- Retain relevant evidence (such as call logs, emails, or screenshots) of any unauthorized futures contract trading incidents and report to the Hong Kong Police Force.

Common Investment Scams

- Beware of fake financial institutions or investment advisors. Scammers may impersonate company employees, regulatory agencies, or "investment experts" to cheat into providing account information or making transfers via phone, email, or social media. Never fall for "high-return, zero-risk" investment advice.

- Beware of fake websites. Verify the website URL (e.g., HTTPS encryption and official domain name) and avoid phishing websites. Always confirm the correct website URL, especially before logging in your account. Phishing websites often use similar URLs to deceive users.

- Beware of fake websites and counterfeit apps. Only download mobile apps from official websites or app stores. Avoid clicking on unidentified links. Legitimate licensed corporations will not ask customers to log in or transfer funds to personal accounts through unidentified links.

- Beware of social engineering scams. Do not share your financial or personally identifiable information on social media or public platforms. Always beware of calls or messages claiming to have "won a prize," "account issues," or "urgent operations." Scammers often create panic to trick you into disclosing information. If you have any questions, please contact our customer service hotline at 3768 9988.

"Anti-Fraud Detector" and the "Anti-Fraud Detector App" mobile application

- The users can search the "Anti-Fraud Detector" database to verify whether websites, phone numbers, security, and other information may be involved in a scam with using the "Anti-Fraud Detector" and the "Anti-Fraud Detector App" mobile applications. The "Anti-Fraud Detector App" can also send instant alerts if it the users are directed to potentially fraudulent websites. For more information, please visit below "Cyber Defender" website.

For information on cybersecurity threats and scams, please visit the following websites:

✧ **Cyber Defender** https://cyberdefender.hk/en-us/
✧ **Anti-Fraud Coordination Centre** https://www.adcc.gov.hk/en-hk/home.html
✧ **Investor and Financial Education Council** https://www.ifec.org.hk/web/en/index.page
✧ **SFC Alert List** https://www.sfc.hk/en/alert-list

09/2025