Safety notes for online trading service

Dear Valued Customer:

In view of the increasingly sophisticated technology crimes and cyber-attacks, to protect your account security, we recommend you to take the following measures to protect your online activities:

I. About Login Password

Set a strong password with at least 8 or more alphanumeric characters (including a mix of alphabetic characters, numerals and special characters). Change it regularly (at least once every 60 days) and avoid recycling the same password.

Don't store your password in computers, mobile phones, or electronic devices, and don't use a single password for all your accounts e.g. email account or security trading account. Activate the auto-lock function to prevent unauthorized access.

Don't disclose the login ID and password of your online account to any person (including our staff or Relationship Manager, Account Executive or our Customer Services Department), or respond to any unverified request. Please contact your Relationship Manager, Account Executive or our Customer Services Department if in doubt.

II. Use of Computers & Mobile Phones

Use trusted and secured computer or mobile phone, electronic device for online trading. Log out website or trading system after finishing your trade immediately. Don't use public computer, or unknown and insecure network connection e.g. public WIFI to access your online account

Disable the 'Auto Complete' function to avoid auto form filling by browsers when you input credentials. You can open the browser and go 'tools' – 'Internet Options' – 'Content' – 'AutoComplete Settings', uncheck 'User names and passwords on forms'.

III. Delta Asia Securities Website and Apps

Type the URL (Delta Asia website: www.delta-asia.com) or use a bookmark to enter our online trading website, or Delta Asia Online trading software (PC version) or Delta Asia Mobile trading App (iOS or Android APK). Avoid access the website through hyperlink embedded in e-mail, internet search engine and suspicious pop-up window.

IV. Login Process

When you log in, make sure there is no one is around to watch your login name and password on screen.

Be aware of any counterfeit website (embezzle the contents and images of our official company website) with the possible intention to undertake fraudulent activities or cybercrime. NOT to log in your online account when there are unusual pop-up screen or window, or abnormal slow computer response, and when unexpected steps or information are required. Please notify your Account Executive or our Customer Services Department immediately.

V. Review Account Transactions & Watch Out Personal Information

Keep a close eye on all trade record and balance of your online account. Log on your online account regularly, or when you receive e-statement alert from Delta Asia, to review all transactions promptly. Please notify your Relationship Manager, Account Executive or our Customer Services Department immediately if there is any suspicious or unauthorized transaction.

Please beware for any unauthorized changes to your account information such as mobile phone number, email address and login password, etc.

VI. Secure Systems & Software

Use the latest versions of operating system, internet trading app, software and browser. Keep software up-to-date. Do not 1.) Jailbreak [1]or 2.) Root [2]your mobile phones or electronic devise.

VII. Beware of Computer Viruses

Do not download or open any doubtful files, browse suspicious websites or click on the hyperlinks and attachments in suspicious sources.

Adopt reputable anti-virus, anti-spyware and anti-malware programs and update them as and when they are released; set up a personal firewall.

Consider the data security and privacy before you download and install any software and apps into your computer or mobile phone, electronic device. Only download and upgrade the software and Apps from official App Stores, App Market or reliable sources.

VIII. Network Functions

Using encrypted Wi-Fi networks and remove any unnecessary Wi-Fi connection settings. Don't perform any transactions at machines for public use or with unknown and insecure network connection. To lower the risk, we recommend you to turn off functions allowing mobile payment and NFC functions when you are accessing online account.

---

[1] *Jailbreaking is the process of removing hardware restrictions imposed by iOS, Apple's operating system, on devices running it through the use of software exploits.*

[2] *Rooting is the process of allowing users of smartphones, tablets and other devices running the Android mobile operating system to attain privileged control (known as root access) over various Android subsystems*