Online Security Awareness Guidance

General Risk Disclosure on Use of Electronic Facilities

Due to the nature of the internet, transactions and communications made over the internet may be subject to interruption, interception, transmission blackout, delayed transmission and incorrect data transmission you should be aware that the internet is not a completely secured transmission medium and there may be risks, delays or failure in the course of transmission.

The online trading facilities made available to you for trading in capital markets products are supported by computer-based component systems for the order-routing, execution, matching, resignation or clearing of trades. As with all facilities and computer systems, you will be exposed to risks associated with the systems including the failure of hardware and software. The result of any system failure may be that your order is either not executed according to instructions or is not executed at all. Please refer to the Trading Account Terms and Conditions, and Risk Disclosure Statements which you have been deemed to have read, received and retained during your account opening with us (i.e. Haitong International Securities (Singapore) Pte. Ltd., Haitong International Asset Management (Singapore) Pte. Ltd. and/or Haitong International Financial Products (Singapore) Pte. Ltd.) ("Company") for more information.

We endeavour to put in place high standards of security to protect your interests. Regardless of any security measures taken by us, you have authorised our Company to amongst others accept, rely and act on the electronic transmission given or purportedly given by you to our Company, and our Company shall assume no responsibility whatsoever for any loss or expense resulting from any and all misunderstandings, errors, unauthorised instructions or alterations of instructions, fraud, forgery or forged instructions, operational failures or faults howsoever occurring in the course of the electronic transmission of your instructions.

Guidance on Online Threats

We would also like to take this opportunity to share with you, as our valued client, certain preventive measures that you may take in your business with us to reduce the risks of exposure to online threats such as malware and internet fraud.

Malware is a malicious program designed to gain access to your device without your consent. Once your device is infected, such malware may steal your personal and financial data or utilise your device to conduct other malicious activities.

Internet fraud is generally defined as the use of internet services or software with internet access to defraud victims or to otherwise take advantage of them. Internet crime schemes steal millions of dollars each year from victims and continue to plague the internet through various methods. All persons and organisations, including us and our clients, are vulnerable to fraud.

Beware of Fraudulent Website and Emails

- Please be reminded to be vigilant of the scam known as 'phishing' which makes use of unsolicited emails and/or fraudulent websites to trick the recipient into disclosing confidential personal details such as usernames and passwords, or to trick the recipient into transferring payments to another bank account which were controlled by the scammer. Haitong International's official website is www.htisec.com, and legitimate emails from Haitong International end in the "@htisec.com" domain. If you suspect the website you visit is not our official website, or if you receive any email purportedly from our company requesting for your username and password, or if you receive any call or email purportedly from our company which you find suspicious, please contact our Client Services teams at Singapore (65) 6536 1920 immediately.

- Clients should not access any Haitong International platform or website via the hyperlinks embedded in the emails sent to you from any unknown source or third party as they may likely be from illegitimate sources and potentially 'phishing' attempts.

Version as at 20/11/2024

- Under no circumstance will our Company send emails to clients asking for their account login information, for example, username, password, etc.

- Clients should always stay alert to any possible online frauds to avoid unnecessary loss.

- Clients should always be aware of any "business opportunity", including receiving or holding money for strangers, to avoid falling victim to money-laundering scams.

How to protect yourself?

Keep your personal information, username and password protected

- Never disclose your username or password for any account, whether with Haitong International or other parties, to anyone including our staff. In any case, we will never ask you to disclose such information.

- Avoid using the same login details which you use to access other web services, such as internet site, email etc.

- Take the following precautions as regards to your username and password ("credentials"):

  - credentials should be strong with at least 8 characters of alphanumeric and special characters mix;

  - credentials should not be based on guessable information such as username, personal name, personal telephone number, birthday or other personal information;

  - credentials should be kept confidential and not be divulged to anyone;

  - credentials should be memorised and not be recorded anywhere;

  - credentials should be changed regularly or immediately when there is any suspicion that it has been compromised or impaired; and

  - the same password should not be used for different websites, applications or services, particularly when they related to different entities.

- Usage of multi-factor authentication is strongly recommended.

- Never write down your username and password or reveal the same to anyone or suspicious websites.

Do not share your personal information publicly on social media.

Keep your personal computer protected

- Set a strong password to prevent unauthorised access into your computer

- Install and regularly update anti-virus software, anti-spyware software, spam filters, personal firewall and security updates for browsers to protect your computer from viruses and malicious programs.
- Strengthen your operating system security settings if you access any online banking or trading services and accounts via public wireless network.

- Ensure that all software on your system is up-to-date with relevant security patches. In particular your operating system and your browsers should be prioritized (MS Windows Update or Software Update on Mac OS).

- Do not disable the personal firewall on your operating system.

- Do not install software or run programs of unknown origin.

- Do not open email attachments from strangers, unknown or unverified sources.

Keep your online accounts protected

- Avoid logging on to your accounts using public and shared computers. Make sure no one can see your username and password when you log on to any of your accounts.
- Always log off from the account when you complete using the services or if you intend to step away from your computer. As an additional precaution, your account which is active on the browser application should be logged off.
- Do not connect to unsecured or publicly-available Wi-Fi, to perform financial transactions.
- Always clear the cache and history in your browser and make sure your account information is removed after using any online services.

Update your contact information

Always update us with your latest personal contact information.

Check your account and transaction history details

If you have transacted in your account with us, such as executing buy/sell trades, making deposit/withdrawals or receiving dividends etc, a statement or e-statement will be issued to you. Always check your statements regularly to identify any unusual transactions, and then report any unusual transaction in your statement to us immediately.

Contact us immediately for any suspicious irregularities

If you experience unusual occurrences on your computer or receive unexpected requests via phone or email relating to your account with us, you should contact us immediately. Unusual occurrences on your computer can imply that your computer has been compromised and someone is misusing it, potentially for personal gain. Unusual or suspicious requests from persons claiming to be from Haitong International can imply social engineering or fraudulent activity. Please contact the following immediately should you suspect any irregularities:

✓ Client Services hotline: Singapore (65) 6536 1920

✓ Our Corporate Office at 6 Battery Road #12-04, Six Battery Road, Singapore 049909

✓ Your designated Relationship Manager or Trading Representative

For and on behalf of

Haitong International Asset Management (Singapore) Pte. Ltd.
Haitong International Financial Products (Singapore) Pte. Ltd.
Haitong International Securities (Singapore) Pte. Ltd.