Customer Alert - Beware of Phishing Messages

In light of the increase in phishing cases reported in Hong Kong, East Asia Securities Company Limited ("EAS" or "the Company") would like to remind customers to stay vigilant at all times when receiving communications that claim to represent EAS, including emails and any instant electronic messages (e.g. SMS messages, WhatsApp, WeChat, etc.).

Please note:

- EAS will never send emails or instant electronic messages asking for any sensitive information such as HKID card number, account number, login password, or one-time password ("OTP").

- Beware of communications that claim to represent the Company but were sent from seemingly illegitimate sources, such as email addresses that look similar to the Company's official email addresses.

- EAS will never ask customers to follow or click any hyperlinks to make a transaction.

If you receive any suspicious communications, please call our Customer Service Hotline (852) 3608 8021 (Monday to Friday 9:00 a.m. to 5:00 p.m.) or visit our Company at 9/F, The Bank of East Asia Building, 10 Des Voeux Road Central, Hong Kong. You can also call the Anti-Deception Coordination Centre (ADCC) on (852) 18222 for an anti-deception consultation service provided by the Hong Kong Police Force.

For more security tips, please read the below information.

Security Tips

You are encouraged to read the following information to ensure the safety of your transactions and information.

1. Major Security Tips
2. Use of EAS Cybertrading platform (including Cybertrading and Mobile App)
3. Use of Automated Phone
4. Two-Factor Authentication
5. Fraud Prevention Information
6. More Security Information

1. Major Security Tips

- Never disclose your EAS Cybertrading Platform (including Cybertrading and Mobile App) login number, password, or one-time password to anyone.
- Avoid opening suspicious email attachments, or clicking any hyperlinks embedded in any email, SMS, instant message, social media platform, QR code, search engine, or any untrusted source to access webpages and enter your sensitive information – especially your login details. Only use our online service by typing www.easecurities.com.hk into your web browser, through a bookmarked link, or through EAS' official mobile application.
- If you encounter suspicious calls, online sellers, friend requests, job ads, investment websites, etc., you are recommended to check the account name, payment account, phone number, email address, URL, etc. through the Scameter by clicking on https://cyberdefender.hk/en-us/ to assess the risk of fraud and cyber security before making any transaction.
- Take precautions against phishing scams (such as scams purportedly from government body or financial institution), hackers, viruses, spyware, and other malicious software.
- Always check your SMS/email transaction notifications from the Company in a timely manner, and regularly check your transaction history and statements in EAS Cybertrading Platform (including Cybertrading and Mobile App). Inform the Company immediately in case of any suspicious situations.
- Use official software and keep the operating system and apps installed on your device up to date with the latest security patches. Install anti-virus and anti-spyware software, keep them updated, and scan your device regularly.
- Make your passwords difficult to guess by creating a minimum of eight characters. Avoid using easily accessible personal information such as telephone number or date of birth as your password. Make them different from passwords for other internet services, and change your passwords regularly.
- Never use the same password for different online or social media accounts. If you suspect that someone has learnt your password, it is suggested that you change the password immediately and contact the Company for assistance, if necessary.

2. Use of EAS Cybertrading Platform (including Cybertrading and Mobile App)

- Be alert of your surroundings before logging in. Make sure no one sees what you enter and log off properly after use.
- Download EAS' official mobile application from an official app store (e.g. Google Play or App Store) and do not use the app on any "jailbroken" or "rooted" devices to ensure secure transactions.
- Change your Personal Identification Number ("PIN") immediately when using your online service for the first time and destroy any documents containing your PIN.
- Take note of your last login date and time or "Identity Message" every time you log in to one of our EAS Cybertrading Platform (including Cybertrading and Mobile App).
- If your mobile phone number and/or email address recorded in the Company has been changed or become invalid, visit the Company, any BEA branches, or login to the EAS Cybertrading Platform – Cybertrading to update your personal information.
- Set up auto-lock, passcode lock, and enable remote wiping to prevent unauthorized access. In the event of loss/theft, it is recommended to change your EAS Cybertrading Platform (including Cybertrading and Mobile App) PIN by logging into EAS Cybertrading Platform (including Cybertrading and Mobile App) and deactivate your i-Token, if applicable.
- Notify the Company immediately of any actual or suspected unauthorised access of your account.

- Protect the computer and mobile phone you use for logging into the EAS Cybertrading Platform (including Cybertrading and Mobile App). If your device is capable of biometric authentication (such as fingerprint or facial recognition), do not disable any features that strengthen the security of biometric authentication and do not let any other person register his/her biometrics on it.
- You should not use facial recognition for authentication if you have identical siblings or siblings that look like you, or if you are an adolescent with rapidly developing facial features.
- Do not use a public computer or public/unknown Wi-Fi network to access online services. Make sure to use an encrypted network when logging in to online services through Wi-Fi, and remove the settings of any unnecessary Wi-Fi connections. Disable wireless network functions such as Wi-Fi, Bluetooth, NFC, etc. when not in use.
- Avoid using online services through free or untrusted Virtual Private Networks ("VPNs"). If you need to use remote access technology to access online services, please use trusted software without publicly known vulnerabilities.
- Carefully read the installation and/or permission requests from websites, apps, and other software and programs. Do not install or run apps from third-party/untrustworthy sources on your device, and uninstall any suspicious apps.
- Regularly check and update your system's web browsers and any of EAS' official mobile application on your devices.
- Be alert if using public USB charging stations for your mobile phone or device to avoid malware infection.
- Do not submit documents (such as scanned identity documents, bank statements, or letters) to any untrusted website or app.

3. Use of Automated Phone Service

- In order to prevent fraud, please keep your Automated Phone PIN secret.
- Never disclose your Automated Phone PIN to anyone (including EAS staff or police officers).
- Do not allow anyone to use your Automated Phone PIN to perform enquiries/transactions.
- Update your Automated Phone PIN regularly to ensure safety.

4. Two-Factor Authentication

- The Company provides a two-factor authentication service for its e-Channels to enhance security for online transactions. You are required to use i-Token[*] or enter the OTP[#] sent by the Company when you log in.
- Safeguard your devices for two-factor authentication. Do not leave your security device (including your mobile phone which has i-Token activated or receives OTP SMS) unattended or allow anyone to possess or control your security device.
- Do not share any OTP sent to your mobile phone with other people.
- Do not install i-Token on any "jailbroken" or "rooted" devices.

[*] You are required to register your mobile phone number with the Company before you can register and use i-Token.

[#] OTP SMS cannot be forwarded to any other phone number, even if you have enabled the "SMS forwarding" service with your mobile phone service provider in Hong Kong.

5. Fraud Prevention Information

- If you have any suspicions about the identity of any apparent intermediary/representative who promotes EAS products or services, you should immediately make a call to the Company through official channels to verify their identity.
- Notify the Company immediately if you lose and/or subsequently replace any identity documents which you registered with EAS when opening your account, or if you have any suspicion that your personal information, statements or account details may have been compromised or stolen.
- Beware of bogus SMS messages and voice message calls. If you are suspicious about the identity of any callers, call the Company immediately through official channels to verify with the Company.
- Beware of fraudsters who impersonate staff of the Company, and unauthorised share-trading transactions. If you notice any suspicious or unauthorised activity related to your account, you should make a call through an official channel and verify with the Company immediately.
- To avoid being deceived by a message, verify the sender's identity through alternative channels before taking any action.
- Look out for common signs of a phishing email, such as a malicious sender address, subject heading with a “warning” or “FYI” label, a request that you enter personal information or click on a suspicious link, generic salutation, threat or false sense of urgency, demand for sensitive information or instruction to open an attachment, or poor spelling/grammar. In any such case, please verify the sender’s identity through alternative/official channels or delete the message immediately.
- Before entering the OTP, please ensure the website is trustworthy.
- Protect all mobile devices you own which can be used to access EAS’ official mobile application, and prevent others from accessing it.
- Pay attention to the anti-deception materials and the latest news issued by Hong Kong Monetary Authority, Hong Kong Police Force, or other authorized institutions.

6. More Security Information

To learn more about security issues, please click the following links:

Hong Kong Police Force:

- Beware of Technology Crimes
- What is Phishing Attack
- What is Online Account Hijacking?
- What is WhatsApp Hijacking?

Anti-Deception Coordination Centre's anti-scam videos/alerts (in Cantonese with English caption)

- Latest Scam Alerts
- A-Shares Investment Fraud
- Telephone Deception
- Emotional Disturbances Faced by Scam Victims
- Internet Investment Scams
- Celebrity Investment Scams
- Romance Scams cum Investment Scams
- Online Employment Scams
- Phishing SMSes/ Websites

HKSAR Government:

- Cyber Security Information Portal
- InfoSec

Hong Kong Monetary Authority:

- Protect your Personal Digital Keys, Beware of Fraudulent Links! - Credit Card
- Protect your Personal Digital Keys, Beware of Fraudulent Links!
- Smart Tips on Using Net Banking Services
- Smart Tips on Using ATMs
- Smart Tips on Protection of Personal Digital Keys
- Smart Consumers Beware of Fraudsters!
- Scameter, Scan for Scam

If you notice any suspicious transactions or receive suspicious transaction notifications, please call our Customer Service Hotline (852) 3608 8021 (Monday to Friday 9:00 a.m. to 5:00 p.m.) or visit our Company at 9/F, The Bank of East Asia Building, 10 Des Voeux Road Central, Hong Kong. You can also call the Anti-Deception Coordination Centre (ADCC) on (852) 18222 for an anti-deception consultation service provided by the Hong Kong Police Force.