POEMS Online Trading Securities Guidelines

Your Role In Safeguarding Your Personal Data And Account Information

1. **Managing your password**

    - Passwords must never be shared or revealed to anyone else besides the authorised user. The authorised user will bear all responsibility for any actions taken by the other party.

    - For security reasons, please note that PhillipCapital will not make unsolicited requests for your information through email or on the phone unless it is initiated by you; under no circumstances would PhillipCapital ask you to reveal your password.

    - Users are advised not to store the password in paper or in any electronic means in case of exposure. Writing the password on a post-it and sticking it to the computer screen is strictly prohibited.

    - Do not use the same password for Phillip Securities accounts as for other non Phillip Securities access (e.g., personal ISP account, option trading, benefits, etc.).

    - If someone demands a password, do not disclose it.

    - Do not use the "Remember Password" feature of applications (e.g., Outlook Express, Netscape Messenger).

    - Ensure that no one can see your Password when you log in to our system.

    - Memorise your Password and do not record it anywhere

    - Change your Password regularly

    - If an account or password is suspected to have been compromised, change your password and inform the incident to POEMS customer service officer at 6531 1555

    It is strongly recommended that passwords should have the following properties:

    - All passwords must have at least eight (8) characters.

    - All user-chosen passwords for computers and networks must be difficult to guess.

    - All user-chosen passwords are best recommended to be alphanumeric.

    - Passwords should not be of the following types:

1. dictionary words
2. derivatives of userids and names
3. common character sequences such as "123456"
4. easy obtainable information of the user such as spouse's name, license plate, passport number, social security number, and birthdays etc

2. Log Out when not in use

Always remember to logout of your online trading session when you have completed your online trading transactions or when you need to walk away from your computer even for just a while. Do not leave your computer unattended while online trading transactions are being processed.

3. Email Security

It is important that you do not give your account no or password and other confidential information in your enquiries and/or comment, as email information is not encrypted during transmission.
If you encounter any suspicious email, passing off as an email from POEMS or Phillip, please notify us immediately at (65) 65311555.

4. Alert on Phishing

Recently, there are many cases of fraud connected with the scam known as 'phishing'. The scam makes use of unsolicited emails and/or fraudulent websites to trick people into disclosing confidential personal details such as user-names and passwords.

Techniques used include, but are not limited to,

- Using false email address, logos and graphics to mislead people into accepting the validity of emails and websites;

- Faking domain names to appear as if they represent the actual companies.

- Duping people into providing personal details through one or more methods such as hyperlinks to fake websites or embedded forms in emails.

5. Securities Measure to prevent keystrokes being captured

You can take the following precautions:

- Ensure that you install an effective personal firewall as well as anti-virus, anti-spyware and anti-Trojan horse software. These should be updated regularly.

- Do not download any software from a website that is of doubtful origin.

- Do not open any email or attachment that is from a source unknown to you. When in doubt, delete such email without opening it.

6. Clearing your Cache

We strongly advise that you clear your browser's disk cache after each online trading session.
Cache files on a computer can retain images of data sent or received over the Internet, making them a potential target for a system intruder.
You are advised to go directly to the domain name of PhillipCapital www.phillip.com.sg or www.poems.com.sg when logging onto our website; you should not accept links or redirections from other websites or media for the purpose of logging onto our website.

7. Mitigation in Mobile Malware

- Only download and install applications from the official application stores (i.e., Google Play Store for Android). As an added precaution, check the developer information on the application listing, as well as the number of downloads and user reviews to ensure it is a reputable and legitimate application.

- Disable the option to “Install Unknown App” or “Unknown Sources” in the mobile settings.

- Exercise caution when clicking on advertisements embedded within applications that lead to third-party website prompting files downloads.

- Do not grant permission to persistent pop-ups that request for access to your device’s hardware or data.

- Ensure that mobile devices are installed with updated anti-virus/anti-malware applications that can detect and remove malware.

- Regularly update the mobile devices’ operating systems and applications to benefit from the latest security patches.