uSMART Securities
盈立證券

Security Guidance

You play a role in safeguarding your personal and account information. Below are some recommended practices to ensure your information is not compromised:

Password

- Do not share your user ID or password with anyone. Each valid user ID and password identifies you uniquely as one of our valued customers.

- uSMART will not make unsolicited requests for your personal or account information through email, social media or on the phone unless it is initiated by you; under no circumstances would uSMART ask you to reveal your password.

- You are advised not to store your password on paper or in any electronic means.

- Change your password regularly.

- All passwords must have at least 8 characters.

- Password should preferably be:

    - Alphanumeric.
    - Words that are not found in dictionary.
    - Common character sequences such as "abcd".
    - Easy obtainable information of yours such as date of birth, family member's name.

Transmission over the Internet

Due to the nature of the Internet, transactions may be subject to interruption, interception, transmission blackout, delayed transmission and incorrect data transmission. Regardless of any security measures taken by uSMART, uSMART shall assume no responsibility whatsoever for any loss or expense resulting from such delays, interruptions and/or interceptions.

Messages sent to uSMART over the Internet cannot be guaranteed to be completely secure. uSMART will not be responsible for any damages incurred by you if you send a message to over the Internet.

Phishing

It is critical to take precautionary measures against cyber frauds. Examples of phishing techniques used include, but are not limited to:

- False email address, logos and graphics to mislead you into accepting the validity of emails and websites.
- Fake domain names, hyperlinks, embedded form which appear as if they represent uSMART.
- Other methods designed to mislead you or trick you into providing personal details, such as uSMART user ID or password, or any other sensitive information or downloading a virus.

Website

uSMART does not represent or warrant that:

- uSMART website will be available and meet your requirements.
- Access will not be interrupted.
- No delays, failures, errors or omissions or loss of transmitted information.
- No viruses or other contaminating or destructive properties will be transmitted or that no damage will occur to your computer system.

uSMART will not be responsible in any manner for direct, indirect, special or consequential damages arising out of the use of uSMART website. uSMART make no representations or warranties regarding the accuracy, functionality or performance of any third party software that may be used in connection with uSMART website.

You have sole responsibility for adequate protection and back up of data and/or device and for undertaking reasonable and appropriate precautions to scan for computer viruses or other destructive properties.

Contact

If you encounter any suspicious email or any email/social media posting impersonating anyone from uSMART, please notify us immediately at +65 63030663 or support@usmart.sg. It is important that you do not give your uSMART ID, user ID or password and other confidential information in your enquiries and/or comment, as email information is not encrypted during transmission.