SECURITY PRACTICES TO SAFEGUARD YOUR PASSWORD

Customers are advised to adopt the following:

- **Do not** reveal your Password to anyone. Under no circumstances will you be required to reveal your Password to a iFAST staff.
- **Select** a unique Password that is different from your other personal numbers like your phone or date of birth.
- **Try** not to use sequential numbers (eg. 123456) or the same number more than twice (eg. 121145) for your Password.
- **Do not** use your Password for other web-based services as they may not be secure.
- **Do not** write your Password down or store it in any computer storage devices. It is best you memorize your Password.
- **Change your Password** regularly.
- **Clear your cache and history** after each login session.
- **Always remember to log off.**
- **When asked** if you want your browser to store your Login Name/Password, always click 'No'.
- **Do not** enter your Password into computer you are not familiar with, like those in your friend's office, or in an Internet café.
- **Install** virus protection software and keep it updated.
- **If** you are using wireless network devices, ensure that the transmission is secure.
- **Access your account** and transaction history regularly to check the details of your holdings.

SECURITY ADVISORY: PHISHING SCAM

Phishing (pronounced fishing) is the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

Common techniques that are used by the phishing fraudsters include, but are not limited to the following:

- Using false email addresses, logos, and graphics to mislead you into accepting the validity of the emails and web sites;
- Faking domain names to appear representing us;
- Duping users into providing personal details through one or more methods such as hyperlinks to fake websites or embedded forms in emails

Customers are advised on the following:

- iFAST will not make unsolicited requests for customer information through e-mail or on the phone unless it is the customers who initiated the contact;
- Under no circumstances will iFAST staff be asking customers to reveal their Passwords;

- Always personally enter the domain **www.ifastfinancial.com.hk** when logging onto our website. Do not accept links or redirections from other websites or media for the purpose of logging onto iFAST.
- When logging in, always ensure that it is a SSL encrypted connection. This is indicated as https:// in the URL or as a padlock in the status bar. Always check iFAST's name in the server digital certificate.
- Always be on the alert for phony websites and suspicious emails purporting to be from iFAST. If you suspect that you are being phished, please do contact us immediately.

SECURITY ADVISORY: SPYWARE ALERT

Spyware consists of computer software that gathers and reports information about a computer user without the user's knowledge or consent. These programs monitor user browsing patterns on the Internet, harvest private information (e-mail addresses, passwords and credit card numbers), and transmits these information in the background to someone else.

Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet. Sometimes advertised as a means to improve internet connection speed and gain other benefits, some spyware, when installed, redirect and reroute the internet connections of users through the spyware servers.

- You may have spyware in your computer if:
- You start getting annoying ads popping up on your screen.
- Your web browser settings have been changed without your knowledge.
- You have a new 3rd party toolbar in your web browser which you are finding it difficult to get rid of.
- Your web browser crashes frequently when you are surfing.
- Slow down in the system performance of your computer where computer operations take longer time than usual.

Customers are advised on the following:

- Do not download and install software from unknown websites.
- Refrain from clicking on banners and pop-up ads that entice you with freebies.
- Install and update anti-spyware software regularly. Perform system scan on your computer to locate, quarantine and delete any spyware in your system.
- Install anti-virus software and keep it updated with the latest virus signatures **(also called virus definition file)**.
- Keep your computer operating system and Web browser current. Perform regular system updates for your operating system.
- Change your Investment Account password regularly.

iFAST treats online security with utmost importance, and as a precautionary measure, we have been actively blocking traffic to iFAST that has passed through redirector/spyware services. If you have at any time been denied access to our website, you may be either intentionally or inadvertently running redirector/spyware software on your computer. In such cases, we urge you to seek professional IT advice or uninstall such software.

Two Factor Authentication (2FA)

What is 2FA?

2FA stands for Two Factor Authentication.

Why do I need to have 2FA to access iFAST platform?

As a continuous commitment to offer maximum security to our online customers, iFAST has introduced the 2FA as an additional layer of authentication.

With 2FA, should your User ID and PIN be compromised for any reason, the ‘intruder’ will also need to have your 2FA, before he can access your iFAST account online. This makes it difficult for hackers who manage to obtain a string of customers' User IDs and PINs via phishing or spyware.