Tips on Online Security

Security Practices to Safeguard Your Password

You 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 an iFAST Financial staff.
- Select a unique password that is different from your personal information such as your telephone number, date of birth or other guessable personal information.
- Your password should be at least 8 characters long and include both alphabets as well as numbers.
- Try not to use sequential numbers (eg. 123456) or the same number more than twice (eg. 121145) for your password.
- Do not use the same password for different web-based services or applications.
- Do not write your password down or store it in any computer storage devices. It is best that you commit it to memory.
- Change your password regularly or when there is any suspicion that it has been compromised or impaired by using the 'Change Password' feature.
- Do not enter your password into computers you are not familiar with, like those in your friend's office, or in an internet café.
- When asked if you want Internet Explorer or other browsers to store your User ID and password, always click on 'No'.

Protecting Yourself Online

- Clear your cache and history after each login session.
- Never leave your session unattended and log off your online session after use.
- Check your last login details and notify us if you notice any doubtful logins.
- Install anti-virus, anti-spyware and firewall software in your computers 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 and report any discrepancy.
- Do not access your account or perform online transactions on a computer or a device which cannot be trusted.
- Remove file and printer sharing in suspected computers, especially when they are connected to the internet.
- Regularly backup critical data. Consider the use of minimal 128-bit encryption technology to protect highly sensitive or confidential information.

- Delete junk or chain emails.
- Do not open email attachments from strangers.
- Do not disclose personal, financial or credit card information to little-known or suspected websites.
- Check that you are using the official iFAST Financial site. You can check by clicking on the "padlock" icon in your web browser and ensuring that the identity of the site is verified as secure.ifastnetwork.com in the server digital certificate.

Security Tips for Mobile Applications

- Download the mobile application only from Apple iTunes. Downloading from websites other than these could lead to mobile applications that are not legitimate.
- Do not hack or modify your mobile device. Doing so can make your mobile device more prone to viruses and malicious software.
- Take extra care in guarding your mobile device. It is more prone to getting misplaced than your computer.
- If the function is available, turn on the password function in your mobile device and make sure that you use a strong one. This function protects your mobile device so that no one else can use it.
- Most mobile devices or smart phones have an "Erase Data" function. If your mobile device has this, always turn it on. This function erases all your data after several invalid password attempts, so your data will not be compromised if your mobile device is lost.
- Install anti-virus, anti-spyware and firewall software in your mobile devices and keep it updated.

Security Advisory - Phishing Scams

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 as if they are representing us;
- Duping users into providing personal details through one or more methods such as hyperlinks to fake websites or embedded forms in emails.

You are advised on the following:

- iFAST Financial will not make unsolicited requests for your information through e-mail or on the phone unless it is you who initiated the contact;
- Under no circumstances will iFAST Financial staff be asking you to reveal your password;

- Always personally enter the domain ifastfinancial.com or ifastnetwork.com when logging onto our website. Do not accept links or redirections from other websites or media for the purpose of logging onto iFAST Financial.
- 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 that the identity of the site is verified as secure.ifastnetwork.com in the server digital certificate.
- Always be on the alert for phony websites and suspicious emails purporting to be from iFAST Financial. If you suspect that you are being phished, please do contact us at 6557-2000 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 transmit 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 is taking longer than usual.

You are advised on the following:

- Do not download or 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 a system scan on your computer to locate, quarantine and delete any spyware in your system.
- Install a virus protection software and keep it updated with the latest anti-virus signatures.
- Keep your computer operating system and Web browser current. Perform regular system updates for your operating system.
- Change your Investment Account password regularly.

iFAST Financial treats online security with utmost importance, and as a precautionary measure, we have been actively blocking traffic to ifastfinancial.com and ifastnetwork.com 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 Two Factor Authentication (2FA) and how does it work?

Two-Factor Authentication (2FA) provides an additional layer of security for verifying an Internet System user's identity thus making it more difficult for online fraud and mischief to occur. With 2FA, Internet System users will be required to provide a unique One-Time Password (OTP) which is unique and randomly generated in addition to the current login ID and password upon each login. The OTP will be sent to your registered mobile phone number via a SMS text message. You are now able to register and start using this added security feature.

Is 2FA compulsory and how will I be affected?

The 2FA feature has already been implemented on our website. There will be a transition period from now till 31st December 2014, during which users can still choose to postpone the 2FA registration. However, from 1st January 2015 onwards, 2FA registration will be compulsory and every login will require a 2FA OTP. While it is not compulsory for users to register for 2FA during the transition period, you are encouraged to register soonest to enjoy a more secured authentication process thus ensuring better protection to your account and transaction details.