



## **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 Capital 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 Capital staff be asking customers to reveal your Password;
- Always personally enter the domain [ifastcapital.com.my](http://ifastcapital.com.my) and [ifastnetwork.com](http://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 Capital.
- 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 Capital. If you suspect that you are being phished, please do contact us at 2149 0600 immediately.