Do not fall prey to SMSes or emails that ask for details about your bank accounts

Do you know that online phishing is one of the most common scams in Singapore? Recent phishing attempts – sent via SMSes or emails – seek to steal confidential log-in and account information from our customers by claiming that their Online Banking or credit card accounts have been locked or suspended. A website is provided for unsuspecting victims to visit to key in their Online Banking log-in credentials or account details.

Please do not fall prey to such scams when you shop or bank online.

Here are some tips on how you can avoid these scams:

Do not disclose your Online Banking Access Code, PIN or One-Time Password (OTP) to anyone over the phone or in an SMS or email, even if they claim to be police or bank officers.

Do not click on the weblinks in SMSes or emails as these may be phishing attempts. To access our website, always type our URL – www.ocbc.com/login – into the browser's address bar or download the OCBC Mobile Banking app via the App Store or Google Play.

Do not disclose card details such as card number, expiry date, CVV or OTP to anyone.

Be alert and carefully check any notifications sent by us. If you are asked to execute or 'authorise' transactions that you were not aware of, do not do so.

When using your credit or debit card:

Report any fraudulent charges shown in your credit card bills to us for investigation immediately.

Do not key in an OTP to authorise payment if you are not making an online purchase. Also, do not be fooled into keying in an OTP to "unlock" or "reactivate" your card.

Notice anything unusual?

Please call us immediately at 1800 363 3333 (or +65 6363 3333 when calling from overseas) if:

- You suspect a fraudulent activity or transaction has taken place in your account. This may include your token, card or account details being compromised.
- You receive an SMS or email informing you that a funds transfer beneficiary has been added to your account or your daily funds transfer limit has been changed which you did not perform.

If you have changed your mobile number or email address recently, please let us know – via Online Banking or by calling us – so we can update our records and send you SMS alerts or email notifications regarding your banking transactions.

It is important that you stay alert and vigilant. Go to http://www.ocbc.com/securityadvisory to learn more about phishing. Familiarise yourself with and protect yourself using these safe banking tips.

Thank you for banking with us. We look forward to serving you again.

OCBC