Phone Scam alert:

Beware of phone calls tricking you to reveal or log in to websites with your banking login credentials to transfer funds. (15 July 2016)

Recent scams focus on tricking customers through seemingly legitimate interactive automated voice messages. Although there are no cases reported at OCBC Malaysia so far, you are strongly encouraged to exercise caution and prudence to protect yourself from such scams.

Here's how they work. Victims receive calls/interactive voice message from fraudsters impersonating representatives or officers from courier companies, banks, customs officers, the police, or government bodies. There are various scams scenarios. In one, the fraudster informs the call recipient that he has a parcel that is being held back as it contains illegal items and that the call recipient is to transfer funds into bank accounts to release the parcel and avoid detention by the authorities.

In another scenario, the fraudster tricks the call recipient into divulging personal information. For example, the call recipient will be led to a webpage to key in his or her full name, passport details, NRIC number, date of birth and/or Velocity@ocbc (business internet banking) log in credentials (eg. Organisation ID, User ID, Password). In another scenario, the call recipient will be instructed to buy an Android smartphone to download an app/software that prompts him or her to enter personal information and online banking credentials.

Fraudsters can also disguise SMS messages or phone calls as from banks to compel the recipient to transfer funds to a fraudulent bank account to avoid penalty and confiscation. The fraudster may also frighten the call recipient into believing that there are illegal funds in his or her bank account and advise them to transfer these funds to another bank account to avoid being implicated.

Please note that while OCBC Bank may in certain instances contact customers either through automated messages or SMS, we will NEVER ask or direct our customers to provide or input any banking login information to websites not associated with OCBC Bank.

We advise you to stay vigilant and take the necessary precautions at all times. We recommend adopting these security practices to protect yourself.

What you should do:

- Ignore the calls from unsolicited callers. Scammers may use Caller ID spoofing technology to mask the actual phone number and display a different number. Calls that appear to be from a local number may not really be made from Malaysia. If you receive a suspicious call from a local number, hang up, wait five minutes, then call the number back to check the validity of the request.
- Ignore any instruction to transfer funds locally or overseas. OCBC will NEVER call customers to transfer funds to any bank account.
- Do not divulge any personal/bank/login information or transfer funds instructed by unsolicited callers.
- Do not reveal to anyone or key in your Organisation ID, User ID, Password or mobile number into suspicious websites or mobile apps.
- Be wary when you are asked to grant **unusual** permissions to mobile applications.
- If you suspect you have received illegal funds, do not deal with it yourself. Inform the bank and lodge a police report immediately.
- Please call us at 1300 88 7000 (within Malaysia) or 603-8317 5200 (outside Malaysia) immediately if you receive such calls or have disclosed your personal or bank information to unsolicited callers.