Security Advisory:

Alert on Business Email Compromise Scam (27 July 2016)

At OCBC Bank, protecting your money has always been our priority. Here are some ways to secure your computer in order to protect your sensitive information (including user id and login passwords) and prevent hackers/fraudsters from gaining access to transfer your monies or payments due to their fraudulent accounts. This is known as “Business Email Compromise”.

Generally, a target will receive an email from the fraudster, who will purport to be the target’s supplier or their senior executive (eg: CFO, CEO, CTO, etc). The fraudster usually uses an email address that is very similar to the email address of the actual supplier. In some cases, the fraudster may access and take over the email account of the supplier or that of their senior executive and instruct the target to transfer the payment to the fraudster’s account. The fraudster may provide justifications such as, the supplier’s regular bank account has been suspended or is undergoing audit to convince the target to transfer to another bank account instead. The target could also be pressurised to make the payment urgently and on a very confidential basis.

Be aware that:

- Fraudsters frequently make contact via email using either a spoofed email account or by hacking into the legitimate account. Be on the lookout for typos or grammatical errors, awkward writing and poor visual designs and other irregularities as well as attachments which may contain malware. A malicious attachment is often designed to infect the computers or steal sensitive information. Do not open or download attachments in suspicious emails and do not reply to such emails.
- Fraudsters may use the names of legitimate companies and use fake email addresses to show a connection to that company (e.g., CEO@gmail.com).
- In order to catch the target off guard, the instruction to transfer funds is requested to be carried out immediately and/or presented as highly confidential transaction on an urgent basis, in order to make the recipient respond more quickly.

Safeguard yourself:

- Be alert and do not provide sensitive information (including username/id, passwords or bank information) or remit money based on the advice of unsolicited callers or emails. Verify and confirm with your payee of any change in payment details and/or bank account details. You should use previously verified bank account and payment details that your payee’s authorised person(s) have confirmed.
- Do not be pressurised. Be suspicious of requests to take urgent action, especially instructions that depart from the norm.
- Carefully scrutinize all email requests for transfers of funds to determine if the requests are out of the ordinary.
- Do not publish your bank account details on your corporate websites or reveal these details to unknown individuals over the phone. This private information can be used fraudulently to trick genuine customers into making payments to alternative accounts.
- Install and maintain the latest anti-virus software on your mobile devices/computer.
- Do not click on hyperlinks, attachments provided in emails or mobile messages (e.g. SMS, WhatsApp) from suspicious or unknown sources.
- 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, business or bank information to unsolicited callers.