

Security Alert on Malicious Trojan (Banker) in Circulation

Dear customers

It has come to our attention that there is a new Trojan in circulation on the internet. This malicious program infects your computer and at the login stage, is able to steal your Velocity@ocbc login information such as your User Name, Password and Organisation ID.

When you attempt to log in to Velocity@ocbc from an infected computer, the Trojan will present to you a page that looks like the Velocity@ocbc login page. Your browser may hang for a period of time and trick you into entering your login details multiple times. The Trojan will then capture the information and send it to the culprit.

The URL to OCBC Bank's official website is <http://www.ocbc.com.my/>. We advise our customers and other members of the public to only log in through this URL.

If you experience the following while on the site:

- a. Multiple prompting to enter your login information
- b. Your computer hangs for a period of time
- c. Indications of suspicious activities in your Velocity@ocbc account, i.e. Adding of Beneficiary unknown to you or unauthorised 3rd Party Funds Transfer to an unknown account.

DO NOT proceed with your online banking activities but alert us immediately by calling 1300-88-7000 / 03-83175200 for OCBC Bank customers or 1300-88-0255 / 03-83149090 for OCBC Al-Amin customers.

If you do suspect that your computer may be infected :

- Do not use it for any internet banking transactions
- Perform an antivirus scan immediately

We advise our customers to be cautious when accessing the internet. These are some of the precautionary measures that you can take :

- Ensure that your antivirus software is up to date with the latest virus signatures
- Frequently scan your computer for viruses/malware
- Do not open attachments or click on hyperlinks from unknown sources
- Avoid visiting websites housing software or other illegal online resources
- Ensure that your operating system is up to date with the latest patches. This helps to tighten vulnerabilities that such malware may exploit
- Refrain from using internet banking facilities on public computers

Protecting your information has always been our priority. To learn more about our privacy and security policies as well as other useful information about online security and tips on protecting yourself from fraud, please log-on to <http://www.ocbc.com/velocity/my/SecurityTips.shtm>