Spyware and Adware

OCBC Bank treats online security with utmost importance and issues this security alert on Spyware and Adware programmes so that you will be better informed on how to protect your business when using the Internet.

Recent news on Spyware reported that some companies are promising faster internet access if the User channels his web communication through these companies' servers and/or installs special programs onto their computer. In doing so, these companies are presented with opportunities to monitor your web behaviour. Some of these companies are even able to decrypt, thus exposing your online communication including encrypted information containing confidential details such as Organisation's ID, User Name, Password and account particulars – even when keyed in at secured websites.

At OCBC, we are committed to provide the highest level of security to our customers. Hence, we strongly advise that you do not access OCBC's Internet Banking through such web services and refrain from installing dubious computer software in your computer, which can be malicious.

What are Spyware & Adware?

Spyware is a software programme that gathers information about a person or an organisation on the Internet without their knowledge. It is normally installed onto someone's computer to secretly gather information about the User.

Adware is a form of Spyware used by marketers to track Internet User's surfing habits and interests for the purpose of customising future advertising material. Adware can monitor information such as the type of sites visited, nature of articles read or the types of pop-ups and banners a User clicks on. This information collected is then used to customise future advertisements targeted to the User, or can be sold to a third party for the same purpose.

Spyware and Adware programmes slow down the system performance of a computer. These programmes use memory and system resources that can cause the system to crash and be unstable. Such software programmes may also have the ability to monitor keystrokes, scan files on your hard drive, change the default home page of your browser, and relay information about your web visits to unauthorised/disreputable third parties who can potentially manipulate the information.

Hence, Spyware and Adware programmes are considered as potential forms of identity theft as they have the ability to invade your online privacy by gaining access to your Passwords and your organisation's confidential transaction information.

How can you protect yourself?

There are products available that can help you detect, monitor and remove Spyware from your computer. Many computer security software suites now come with a standard feature for Spyware detection and removal.

With proper precautions, you can help protect your organisation's account information from harmful programs:

- Be wary of banners, ads and pop-ups while surfing the Internet.
- Refrain from clicking on them no matter how enticing they may appear.
- Avoid downloading programmes and email attachments from unknown sources.
- Downloads may contain hidden programmes that can compromise your computer's security. Never download or open email attachments from unknown senders.
- Keep your computer operating system and Web browser current.

If your computer is more than five years old, its operating system (e.g. Windows 98, OS 7 etc.) may not offer the same level of protection as newer systems. System manufacturers such as Microsoft and Apple provide frequent updates to help make your system more secure.

You may check out their websites: http://www.microsoft.com/security or http://www.apple.com/support/security/

Install and update your computer with the latest anti-virus software. Commercially available virus protection software helps reduce the risk of contracting computer viruses that can compromise your security. These programmes offer the protection against the latest threats – provided you continuously keep the programme updated.

Install up-to-date anti Spyware programme to regularly scan your computer, locate, quarantine and delete any Spyware/Adware in your computer.

Review the terms and conditions when you install free programmes or subscribe to services from the Internet.

Never divulge your Internet Banking Password to anyone, not even to someone who claims to be a staff of OCBC Bank. Your Internet Banking Password is personal and highly confidential. Our staff will NEVER ask for your Password either via emails, in person or over the telephone.

Change your Internet Banking Password on a regular basis.