Tips on How To Protect Your Computer

1. ***Ensure the computer is protected by reliable security software***

You'll need the following key protection:

- Anti-spyware protection
- Personal firewall protection
- Anti-malware protection

a. Install reliable security software on the PC/notebook

Installing a **personal firewall** is extremely important, especially if you are connected to the Internet regularly or permanently (e.g. via broadband connection). The personal firewall can provide safeguards against any form of external attacks.
If you download files, programmes or plug-ins from the Internet regularly, it is essential to protect your computer with **anti-spyware** and **anti-malware programmes** to prevent unwanted tracking, keyloggers and malicious programmes from running in the computer without your knowledge.
If your computer contains highly sensitive or confidential information, you should consider installing encryption software to protect your data.

b. Update your signature files regularly

Ensure that regular updates are performed for your virus definition files and other security patches that are provided by the software.

C, Update your firewall patches that are provided by the software

a. Find out more

You can read about such software at the reputable websites listed below:

- Norton
- McAfee
- Trend Micro

2. ***Backup your critical data on a regular basis***

3. ***Remove file and printer-sharing option(s) on the computer, especially if your Internet access is via cable modem, broadband connection or such similar setup***

Such sharing options may allow spyware programmes or viruses to spread to other computers.

4. ***Sharing of PC/notebook***

Avoid sharing your PC/notebook as spyware programmes or viruses may be downloaded into your PC/notebook without your knowledge.

5. ***Update security patches for Windows and Internet Explorer***

If you are using Windows Operating System (OS) and Internet Explorer, do visit the Microsoft website regularly to check for updates on security patches. You can also click on "Windows Update" under the "Tools" option located on the Internet Explorer.

6. ***Wireless Connection***

If you are using a wireless network connection, ensure that a proper wireless installation is carried out.

7. ***Exercise caution when installing any third-party software that claims to speed up the Internet connections or improve the Internet browsing experience***

Certain third-party software providers may redirect the Internet session through their own servers without the user's knowledge. Any information the user enters on the browser may be transmitted or stored in these servers. Your personal information and privacy may be compromised, and this may include your username and password when you login to any online banking session.

We strongly recommend that you do not install such software, especially on the computer that is used to access online banking for Company Account. For proper security protection, you should install an anti-virus software, anti-spyware, and personal firewall software to safeguard your PC and Internet access.

8. Delete suspicious or unsolicited emails

If you do open any suspicious email, do not open any attachments or click on any links within the message.

Note

We are actively monitoring the situation and will block traffic to www.maybank2u.com.sg that has passed through or are redirected from suspicious service providers to protect our Internet banking customers.
If the user has installed such software, he/she may not be able to access our website and Maybank2u.com.sg. In such cases, we strongly recommend that the user uninstall any such software.

Maybank Singapore Limited (UEN: 201804195C)