

## 安全须知： 2011 09 恶意软件流通安全警示 （2011 09）

尊敬的客户，

请您注意，根据近期的报告显示，近来有木马恶意软件攻击网上银行。这类恶意程序在您登陆时入侵您的电脑并可以盗取您的企业网银-Velocity@ocbc 的登陆信息，例如您的用户名，密码，组织机构识别码及动态密码。这类程序可以禁用杀毒软件并控制您的电脑。

如果您的电脑已经被此类恶意软件感染，以下几种情况下此类病毒将可能盗取您的登录信息：

- 如果您多次反复收到要求您输入信息的对话框
- 如果在一个页面上，您被要求输入的信息比正常登录过程多（例如：虚假屏幕会要求您输入用户名，密码，组织机构识别码及动态密码，这类信息可能会要求您在一个页面上输入。而华侨银行的合法网页只要求您在第一个页面上输入用户名，密码和组织机构识别码）
- 您也可能被指引到一个假的网站以盗取您的登录信息

以下为合法的 Velocity@ocbc 的登录页面

Velocity - Microsoft Internet Explorer provided by OCBC Group

OCBC Bank

Personal Small and Medium Businesses Corporate & Institutional

Language: English | 中文 You are in: Singapore

Internet Banking Banking Investment Cash Management Investment Banking Trade Services Loans Tools & Info Help Centre

Welcome to Login@Velocity

VeriSign

Browser Compatibility Update

Firefox 5.0 Internet browser is officially certified for use with Velocity@ocbc with effect from 02 August 2011.

To ensure maximum compatibility, it is advisable to use the recommended browser platforms and withhold any upgrade until it has been certified for use.

Please refer to the [latest list of compatible browsers](#).

Security Alert

If you have received an email requesting that you click on a hyperlink to verify your Internet Banking Account information and details, do not respond. For more details, please [click here](#). You are also encouraged to read our [online security tips](#) to safeguard your account.

Spyware Alert!

Learn how to safeguard yourself [click here](#)

Problems Logging on?

Upon logging on, if you fail to see the homepage of Velocity@ocbc, it may be due to a Pop-up Blocker installed in your Internet Explorer. Follow this [guide](#) to turn it off and try to logon again after 10 mins.

Login

User Name

Password

Organisation ID

Login

Attention: Security Alert on Malware in Circulation (Sep 2011)

It has come to our attention of new variants of Spyeeye malware in circulation on the internet. This malicious program infects your computer and at the login stage, is able to steal your Business Internet Banking - Velocity@ocbc login information such as your User Name, Password and Organisation ID. [To read more...](#)

IMPORTANT:

Please do not add this page to your Favorites. To add to Favorites, please use <https://bb.ocbc.com>.

REMINDER:

To protect your interest and the integrity of your transactions, please [clear your browser's cache \(and history\) on your browser](#) after you have logged out.

Secured area

[I have forgotten my Password!](#)

[I have problems logging on](#) | [How do I protect my Password?](#) | [FAQ](#)

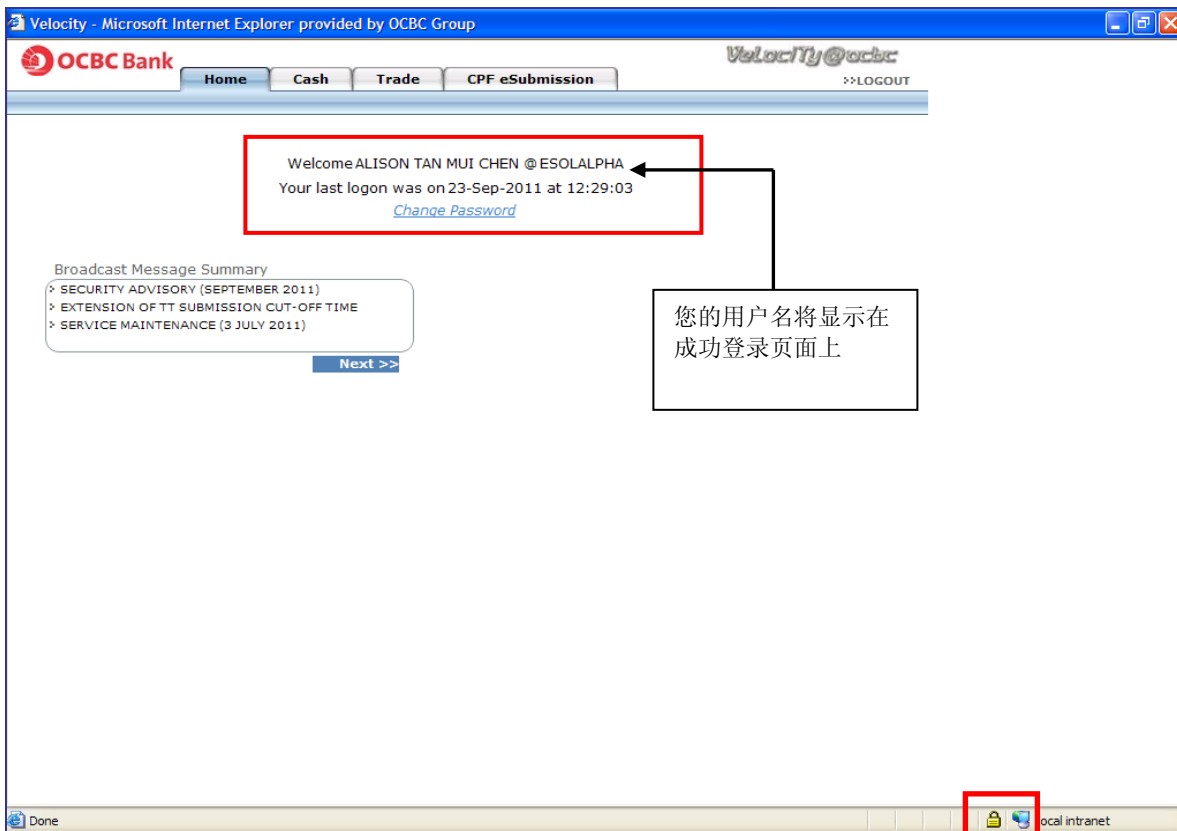
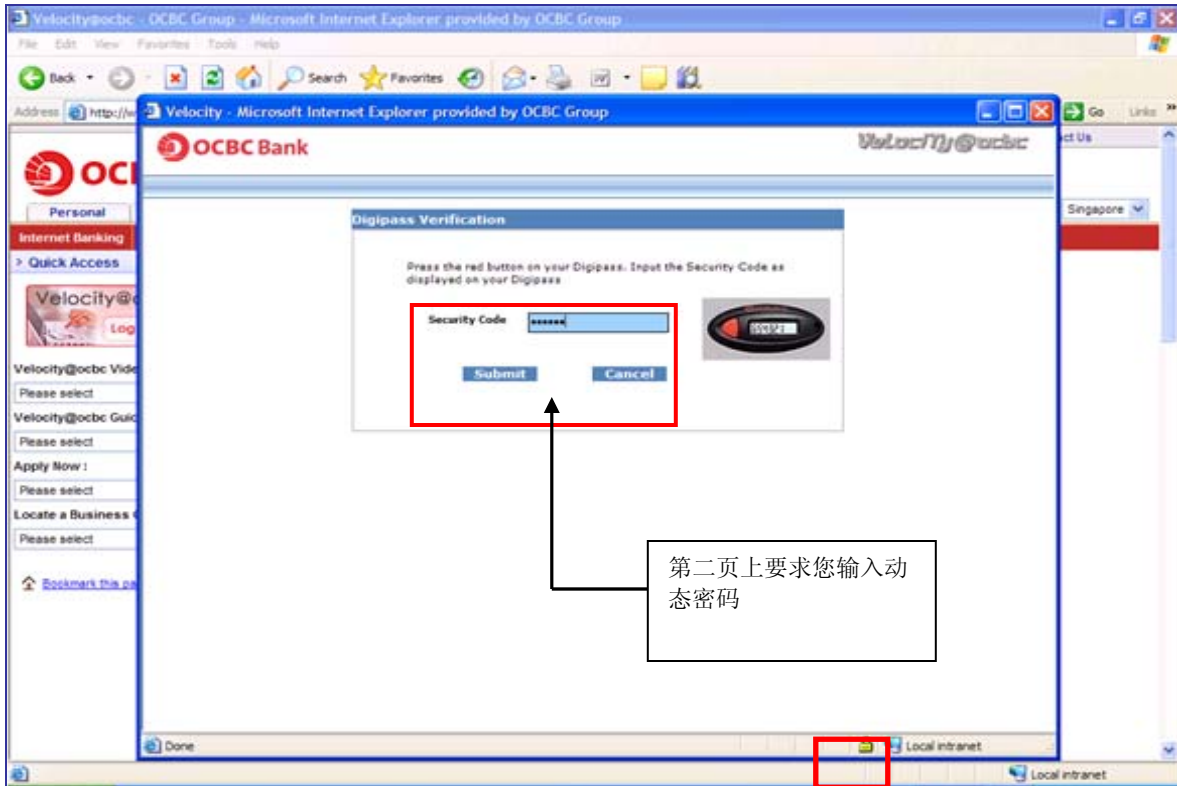
[Velocity@ocbc - "Getting Started" Guide](#)

Applet encryptor started

Local intranet

登录页面无需输入动态密码

安全锁标识表示此网站为安全网站



如果电脑被感染，您可能会被指引到一个假的网站以盗取您的登录信息，如下图所示：



当您进行网银交易时，如果您怀疑您的电脑或者您的银行账户被感染，请您立即致电我们 021-61463222 并立即采取以下步骤：

- 1) 关闭浏览器
  - 2) 确保您的杀毒软件是最新的
  - 3) 开启您的杀毒软件，并全盘扫描您电脑中的文档
  - 4) 如果您的电脑还未安装反病毒软件，请您立即安装最新的杀毒软件并扫描您的电脑
  - 5) 启动运行系统更新：
    - Windows- 开启浏览器> 工具>Windows 更新
    - Macintosh - 点击 Apple 图表（左上角）> 软件更新
  - 6) 重新启动您的计算机并再次登陆到 Velocity@ocbc。如果恶意软件被清除了，您应该不会遇到类似的信息  
在开始网银交易之前，请您立即更改 Velocity@ocbc 登陆密码。
  - 7) 如果您怀疑恶意软件未被成功删除，请您不要再使用这台电脑进行网银交易。请更换另一台未被恶意软件感染的电脑登录 Velocity@ocbc 并更改您的密码。
- 注意：建议授权员电话通知银行重新设置密码。**

我行保证华侨银行 Velocity@ocbc 系统是安全的。但您在做网上银行业务时仍需要保持警惕。您可以使用以下五个提示来防范恶意软件入侵：

请安装杀毒软件保护您的电脑并实时更新杀毒软件签名并定期扫描您的电脑。

- 在输入登录信息前，请您务必使用合法的URL (<https://bbcn.ocbc.com>) 登录网上银行。
- 不要对非您主动提交的交易或请求输入动态密码。
- 避免浏览未知或不安全的网站。
- 不要打开未知或可疑的附件，即使是您认识的人发送给您的。

华侨银行一直将保护您的信息放在首要位置。想要了解更多的有关网络安全和技巧保护自己免受欺诈，请访问以下链接：[http://www.ocbc.com.cn/html\\_chinese/html/velocity/Security\\_Tips.shtm](http://www.ocbc.com.cn/html_chinese/html/velocity/Security_Tips.shtm)