

Security Advisory: September 2011 Security Alert on Malware in Circulation (September 2011)

Dear customers,

We would like to bring to your attention that there have been recent reports of Trojan horse malware attacks on the internet banking websites here. The malware is designed to steal your Velocity@ocbc login information such as User Name, Password, Organisation ID and Security Code. It may also disable anti-virus protection and take over the control of your infected computer.

If your computer is infected by the malware, these are some possible ways the malware will attempt to steal your login information:

- you may receive multiple prompts for login information even when your login information has been entered
- you may be asked to enter more login information on one page than the normal login process (eg. the fraudulent screen asks for your User Name, Password, Organisation ID and Security Code all on the same page, this is different from the legitimate OCBC website that asks only for your User Name, Password and Organisation ID on the first page)
- you may also be re-directed to a bogus site where your login information would be stolen

The following is the legitimate Velocity@ocbc website

Velocity - Microsoft Internet Explorer provided by OCBC Group

OCBC Group | Home | SiteMap | Contact Us

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](#)

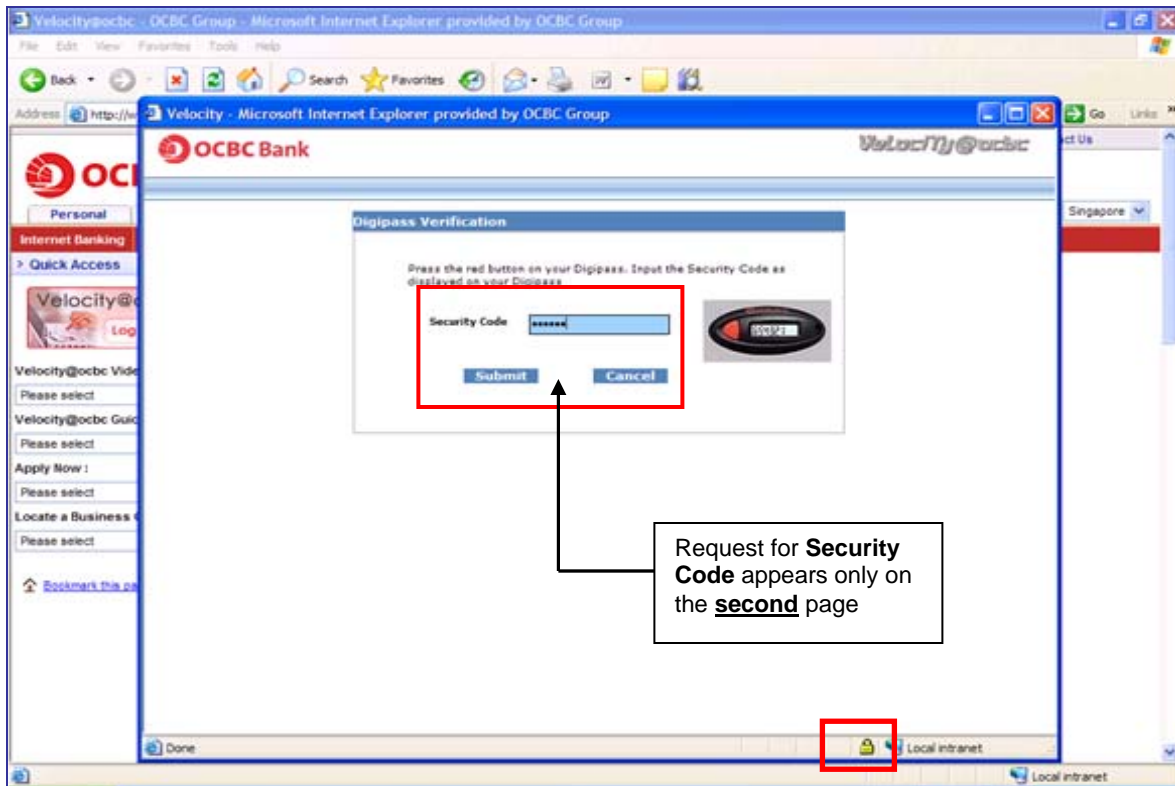
[Velocity@ocbc - "Getting Started" Guide](#)

Applet encryptor started

Local intranet

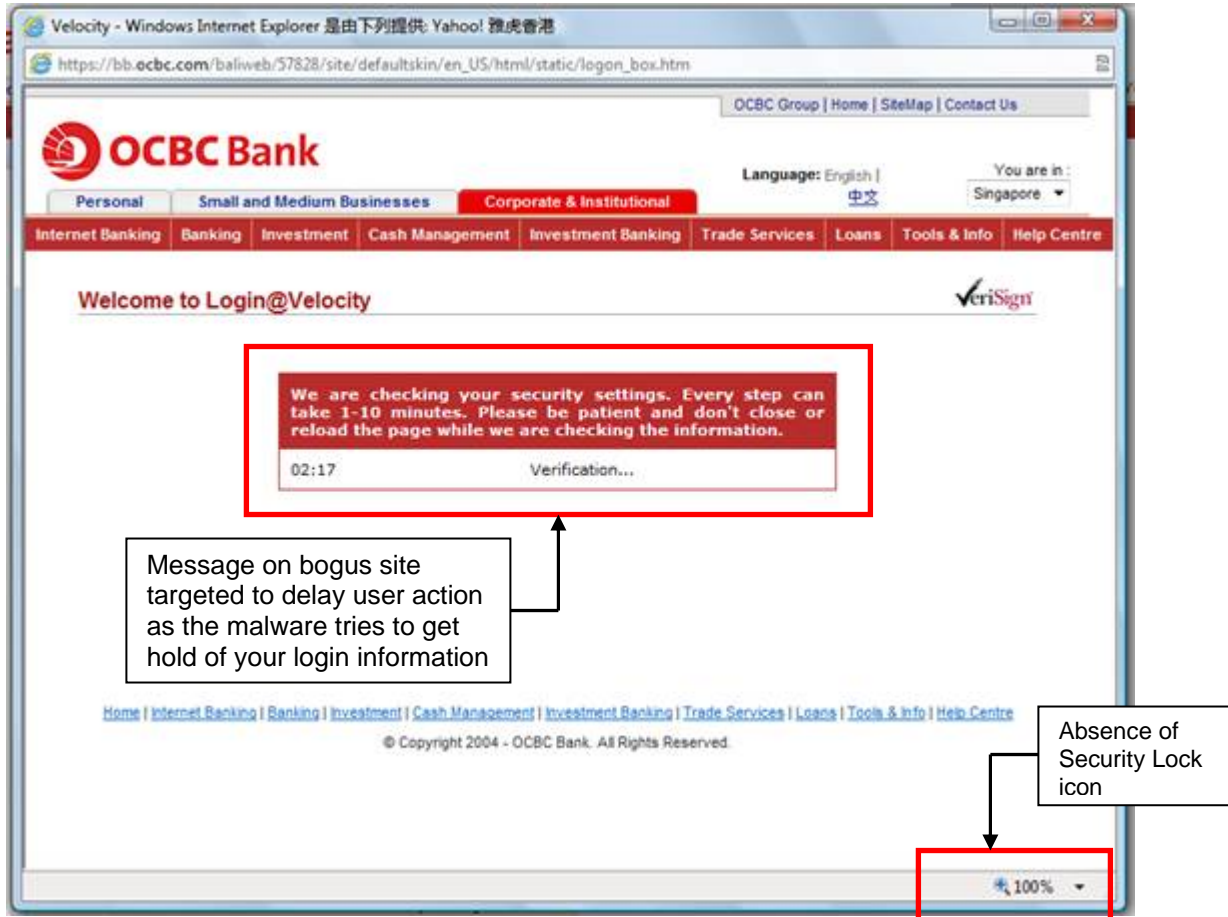
The request for Security Code will not appear on the logon page

Security Lock icon to indicate that this is a secured site



The screenshot shows a Microsoft Internet Explorer browser window displaying the OCBC Bank Velocity portal. The browser title is "Velocity - Microsoft Internet Explorer provided by OCBC Group". The page header includes the OCBC Bank logo, navigation tabs for "Home", "Cash", "Trade", and "CPF eSubmission", and a "Velocity@ocbc" logo with a "LOGOUT" link. The main content area displays a welcome message: "Welcome ALISON TAN MUI CHEN @ ESOLALPHA" and "Your last logon was on 23-Sep-2011 at 12:29:03", with a "Change Password" link below. A red box highlights this message, and a callout box points to it with the text "You will see your user name upon successful login". Below the welcome message is a "Broadcast Message Summary" section with three items: "SECURITY ADVISORY (SEPTEMBER 2011)", "EXTENSION OF TT SUBMISSION CUT-OFF TIME", and "SERVICE MAINTENANCE (3 JULY 2011)", followed by a "Next >>" button. The browser status bar at the bottom shows "Done" and a lock icon next to "local intranet", which is also highlighted with a red box.

Example of an image of a bogus site that you may be re-directed to if your computer is infected :



If you suspect that your computer has been infected by the malware, please contact us immediately at 021-61463222 and follow the steps below:

1. Close the browser.
2. Ensure that your anti-virus software is up to date.
3. Run your anti-virus software and scan your entire computer's files.
4. If your computer is not installed with an anti-virus software, please install with an up to date version immediately and perform a scan on your computer.
5. Perform an Operating System update, for:
 - Windows – Launch Browser > Tools > Windows Update
 - Macintosh – Click on Apple Icon (top left) > Software Update
6. Restart your computer and login to Velocity@ocbc again. You should not encounter the same bogus site again if the malware is completely removed.
Change your password immediately in Velocity@ocbc before proceeding to perform your internet banking transactions.
7. If you suspect that the malware is not successfully removed, please refrain from using the same computer for any internet banking transactions. Login to Velocity@ocbc using another non-infected computer to change your password.
Note: Authorisers are advised to call the Bank to reset their password.

We would like to assure you that our internet banking websites remain secure. You are reminded to stay vigilant when banking online. The following are five tips that you can take note of to protect your computer from being infected with such malware:

Install anti-virus software in your computer, ensure regular updates with the latest virus signatures and scan your computer regularly.

- Always type in the URL (<https://bbcn.ocbc.com>) manually and verify the internet banking website before providing your login information.
- Do not enter any Security Code for transactions that you did not initiate or request.
- Avoid visiting unknown and unsecured websites.
- Do not open unknown or suspicious attachments, even if they are from senders you know.

At OCBC Bank, protecting your information has always been our priority. To learn more about online security and tips on protecting yourself from fraud, please visit: http://www.ocbc.com.cn/html_english/html/velocity/Security_Tips.shtm