



Security Advisory: 15 March 2013
Security Alert on Malware in Circulation (15 March 2013)

Dear customers,

We would like to bring to your attention that there have been recent reports of new malware attacks on internet banking websites. The malware is designed to steal customers' login and authorisation information such as User Name, Password, Organisation ID and One-Time-Password or 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 and authorisation information:

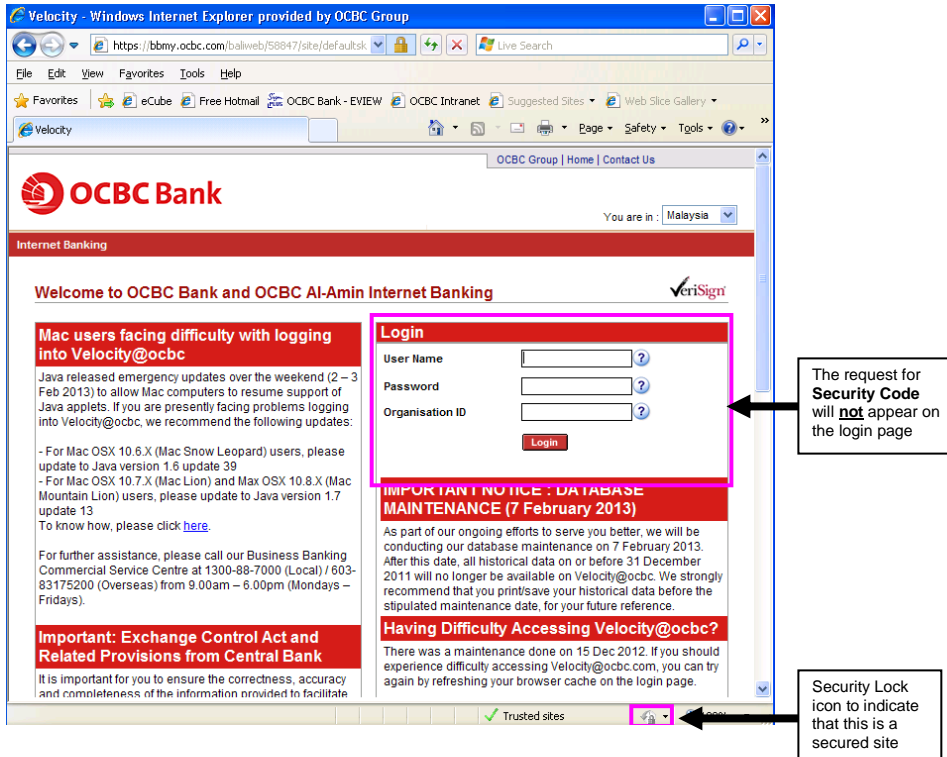
- you may receive multiple prompts for login information even when your login information has been entered
- you may be asked to enter login information on only one page. Eg. the fraudulent screen will ask for your User Name, Password, Organisation ID and One-Time-Password or Security Code all on a single page to gain access to your information faster. The normal login process is done over two pages. The legitimate OCBC website asks only for your User Name, Password and Organisation ID on the first page and your Security Code on the second page.
- you may also be re-directed to a bogus site where your login information would be stolen
- you may be prompted to enter the One-Time-Password or Security Code from your hardware token even if you did not perform any online transactions from your account.

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://bbmy.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.my/business-banking/help-and-support/tips-and-notices.html?>

The following is the legitimate Velocity@ocbc login page



Velocity - Windows Internet Explorer provided by OCBC Group

https://bbmy.ocbc.com/balweb/58947/site/default.asp

OCBC Bank

You are in: Malaysia

Internet Banking

Welcome to OCBC Bank and OCBC AI-Amin Internet Banking

Mac users facing difficulty with logging into Velocity@ocbc

Java released emergency updates over the weekend (2 – 3 Feb 2013) to allow Mac computers to resume support of Java applets. If you are presently facing problems logging into Velocity@ocbc, we recommend the following updates:

- For Mac OSX 10.6.X (Mac Snow Leopard) users, please update to Java version 1.6 update 39
- For Mac OSX 10.7.X (Mac Lion) and Max OSX 10.8.X (Mac Mountain Lion) users, please update to Java version 1.7 update 13

To know how, please click [here](#).

For further assistance, please call our Business Banking Commercial Service Centre at 1300-88-7000 (Local) / 603-83175200 (Overseas) from 9.00am – 6.00pm (Mondays – Fridays).

Important: Exchange Control Act and Related Provisions from Central Bank

It is important for you to ensure the correctness, accuracy and completeness of the information provided to facilitate

Login

User Name

Password

Organisation ID

Login

IMPORTANT NOTICE: DATABASE MAINTENANCE (7 February 2013)

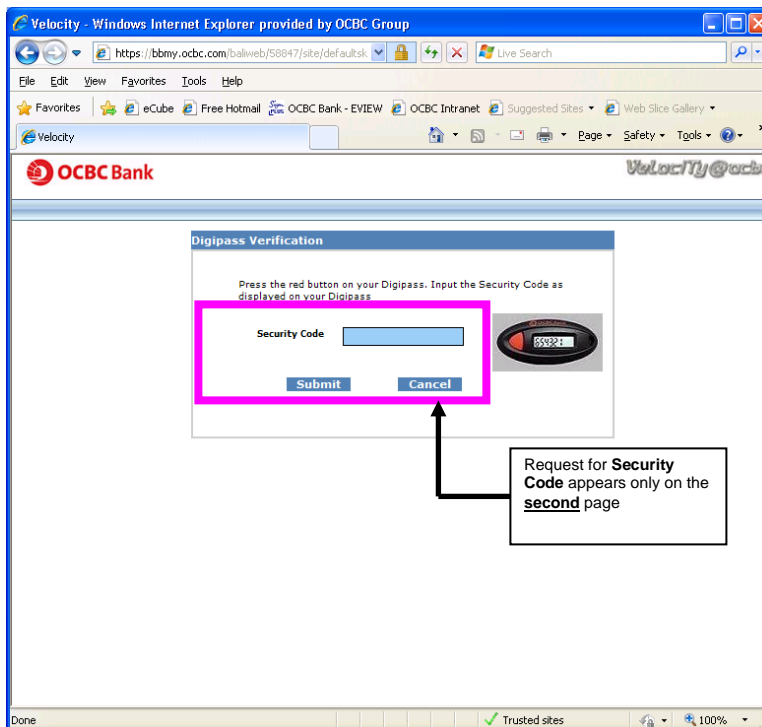
As part of our ongoing efforts to serve you better, we will be conducting our database maintenance on 7 February 2013. After this date, all historical data on or before 31 December 2011 will no longer be available on Velocity@ocbc. We strongly recommend that you print/save your historical data before the stipulated maintenance date, for your future reference.

Having Difficulty Accessing Velocity@ocbc?

There was a maintenance done on 15 Dec 2012. If you should experience difficulty accessing Velocity@ocbc.com, you can try again by refreshing your browser cache on the login page.

Trusted sites

Security Lock icon to indicate that this is a secured site



Velocity - Windows Internet Explorer provided by OCBC Group

https://bbmy.ocbc.com/balweb/58947/site/default.asp

OCBC Bank

Velocity@ocbc

Digipass Verification

Press the red button on your Digipass. Input the Security Code as displayed on your Digipass

Security Code

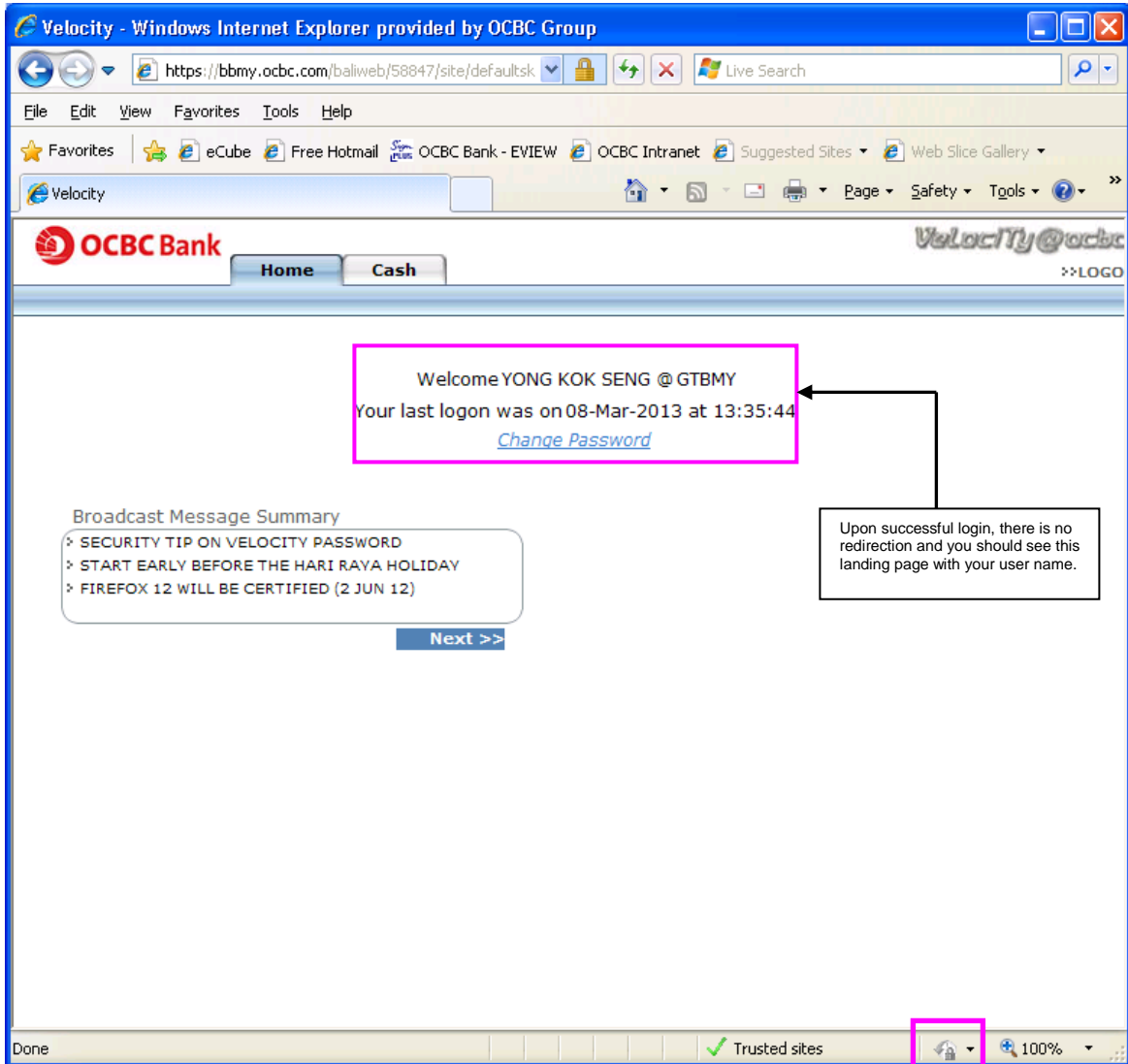
Submit Cancel

Request for Security Code appears only on the second page

Done

Trusted sites

100%



The screenshot shows a Windows Internet Explorer browser window titled "Velocity - Windows Internet Explorer provided by OCBC Group". The address bar shows the URL <https://bbmy.ocbc.com/baliweb/58847/site/defaultsk>. The browser's menu bar includes File, Edit, View, Favorites, Tools, and Help. The Favorites bar contains links for eCube, Free Hotmail, OCBC Bank - EVIEW, OCBC Intranet, Suggested Sites, and Web Slice Gallery. The OCBC Bank logo and "Velocity@ocbc" branding are visible at the top of the page, along with "Home" and "Cash" navigation buttons.

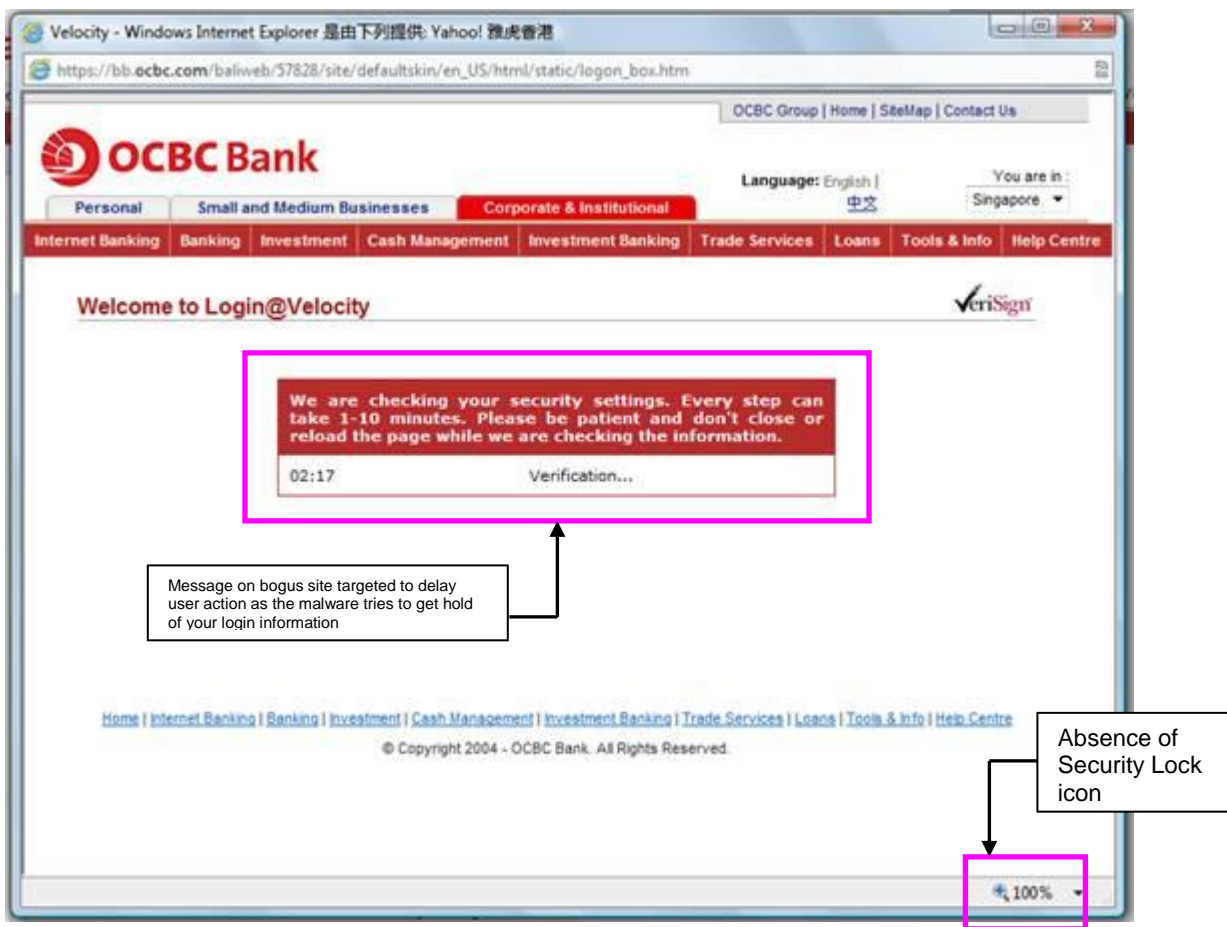
The main content area displays a welcome message for "YONG KOK SENG @GTBMV", stating "Your last logon was on 08-Mar-2013 at 13:35:44" and providing a [Change Password](#) link. Below this is a "Broadcast Message Summary" section with three items:

- SECURITY TIP ON VELOCITY PASSWORD
- START EARLY BEFORE THE HARI RAYA HOLIDAY
- FIREFOX 12 WILL BE CERTIFIED (2 JUN 12)

A "Next >>" button is located below the broadcast messages. A callout box on the right side of the page contains the text: "Upon successful login, there is no redirection and you should see this landing page with your user name." An arrow points from this callout to the welcome message.

The browser's status bar at the bottom shows "Done", "Trusted sites", a security icon (highlighted with a pink box), and a zoom level of "100%".

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



If you experience the above while on your internet banking site, **please DO NOT proceed with your online banking activities 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: To request for a new Login Password, please complete the Velcoity @ocbc User Access request Form and mail to us.

For clarification, please contact us at 1300 88 7000 (or +603 8317 5200 if calling from overseas).