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:

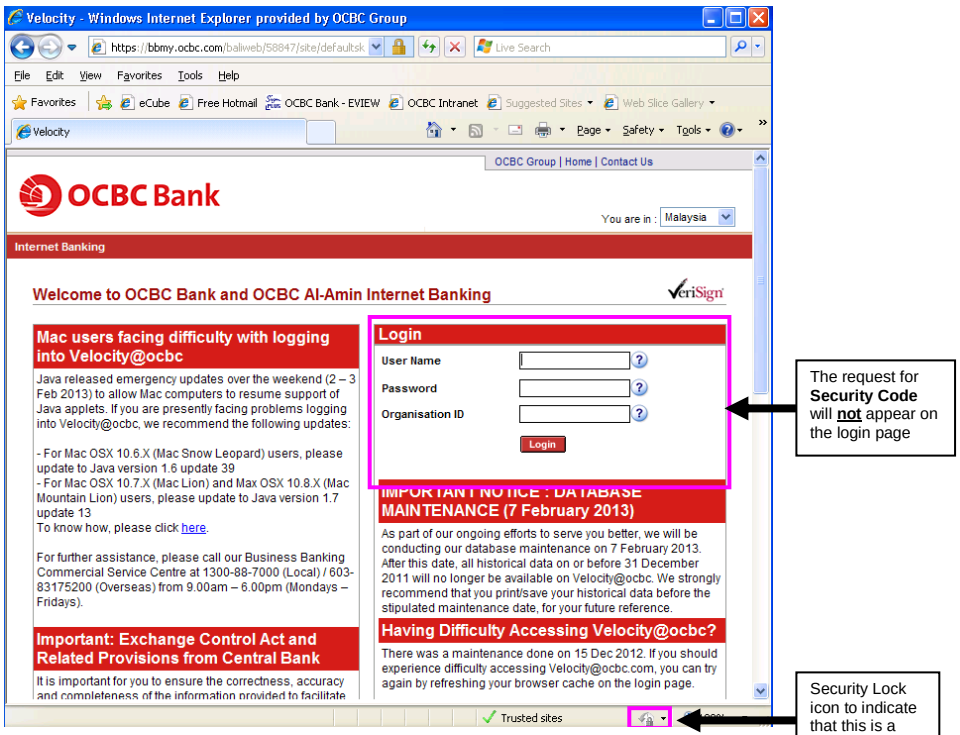
- you may receive multiple prompts for login information even when your login information has been entered
- you may be asked to enter login information on only one page. Eg. the fraudulent screen will ask for your User Name, Password, Organisation ID and One-Time-Password or Security Code all on a single 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.

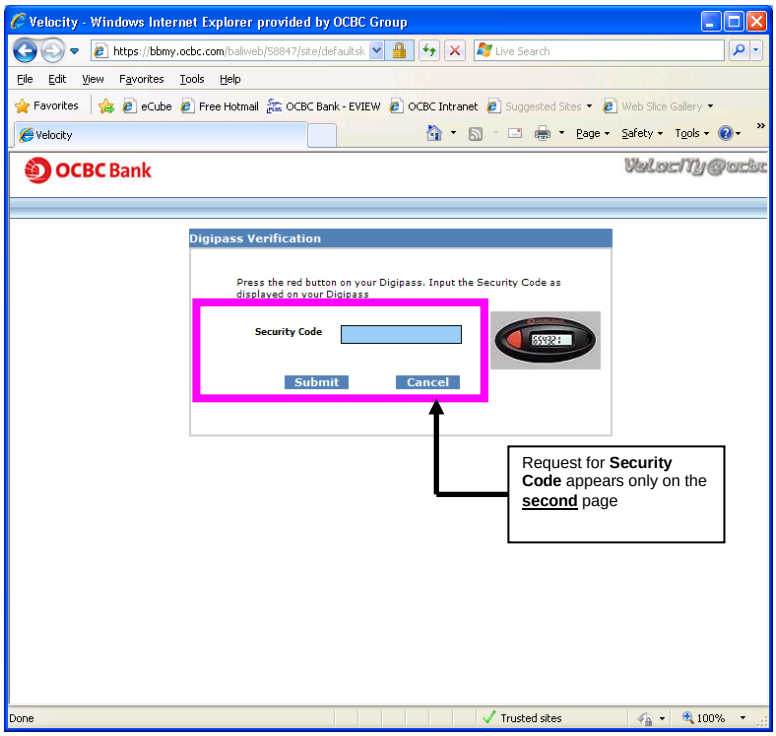
At OCBC Bank, protecting your information has always been our priority. To learn more about online security and tips on protecting yourself from fraud, please visit: http://www.ocbc.com.my/business-banking/help-and-support/tips-and-notices.html?

The following is the legitimate Velocity@ocbc login page

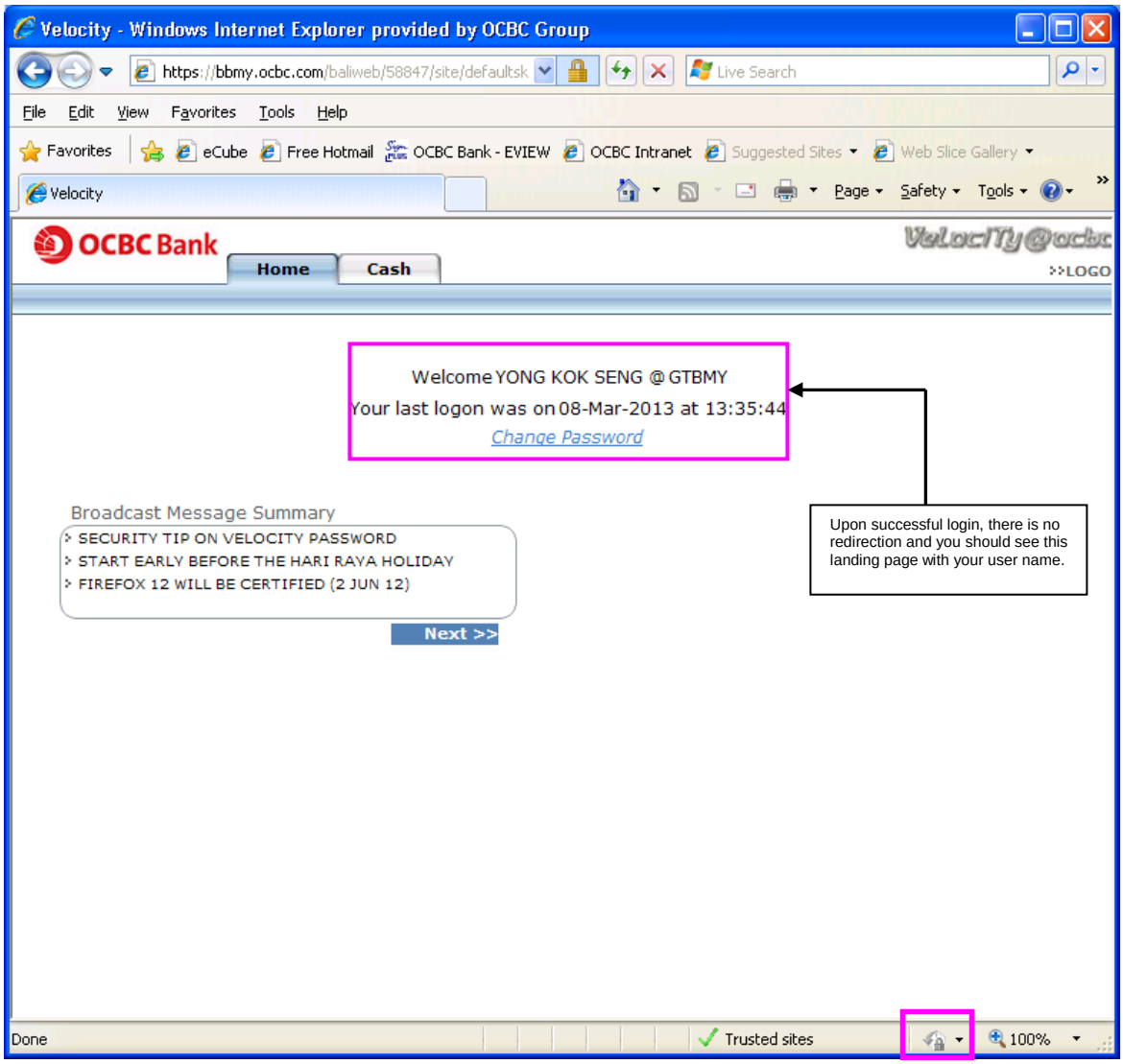


The request for **Security Code** will **not** appear on the login page

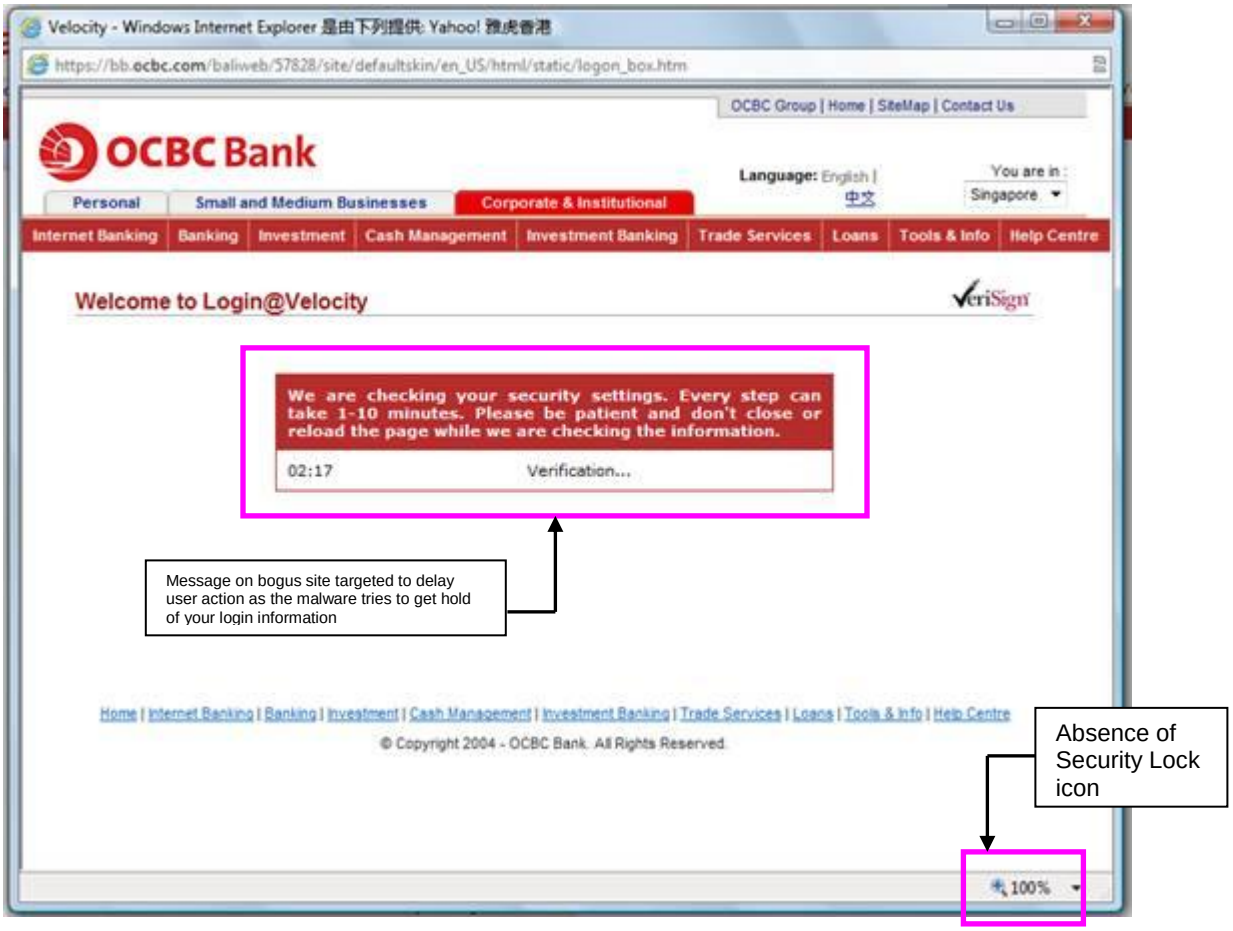
Security Lock icon to indicate that this is a secured site



Request for **Security Code** appears only on the **second** page


Velocity - Windows Internet Explorer provided by OCBC Group
https://bbmy.ocbc.com/baliweb/58847/site/defaultsk
Live Search
File Edit View Favorites Tools Help
Favorites eCube Free Hotmail OCBC Bank - EVIEW OCBC Intranet Suggested Sites Web Slice Gallery
Velocity
Page Safety Tools
OCBC Bank
Home
Cash
VeloCITy@ocbc
>>LOGO
Welcome YONG KOK SENG @ GTBMY
Your last logon was on 08-Mar-2013 at 13:35:44
Change Password
Broadcast Message Summary
SECURITY TIP ON VELOCITY PASSWORD
START EARLY BEFORE THE HARI RAYA HOLIDAY
FIREFOX 12 WILL BE CERTIFIED (2 JUN 12)
Next >>
Upon successful login, there is no redirection and you should see this landing page with your user name.
Done
Trusted sites
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).

March 2013