



Security Advisory: 13 March 2013
Security Alert on Malware in Circulation (13 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:

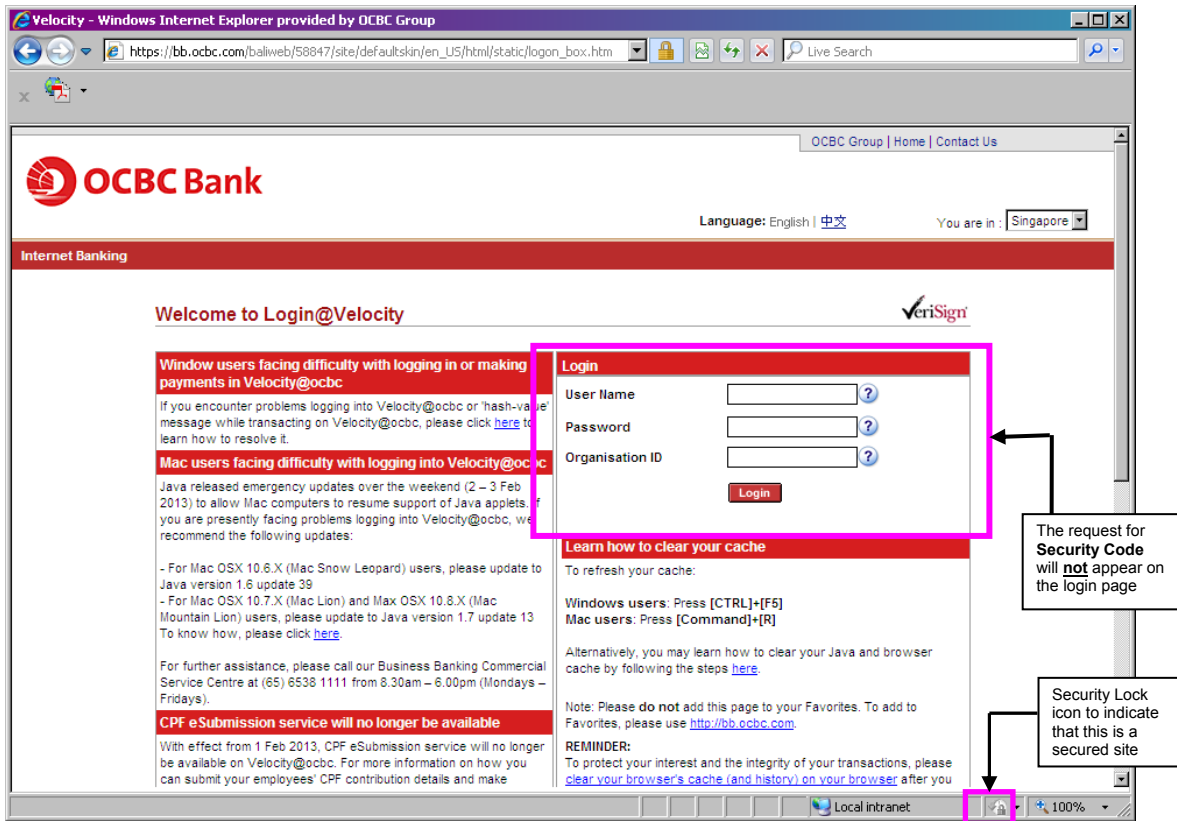
- you may receive multiple prompts for login information even when your login information has been entered
- you may be asked to enter login information on only one page. Eg. the fraudulent screen will ask for your User Name, Password, Organisation ID and One-Time-Password or Security Code all on a single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

The following is the legitimate Velocity@ocbc login page



Velocity - Windows Internet Explorer provided by OCBC Group

https://bb.ocbc.com/baliweb/58847/site/defaults/en_US/html/static/logon_box.htm

OCBC Bank

Language: English | 中文 You are in: Singapore

Internet Banking

Welcome to Login@Velocity

Window users facing difficulty with logging in or making payments in Velocity@ocbc

If you encounter problems logging into Velocity@ocbc or 'hash-value' message while transacting on Velocity@ocbc, please click [here](#) to learn how to resolve it.

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 (65) 6538 1111 from 8.30am - 6.00pm (Mondays - Fridays).

CPF eSubmission service will no longer be available

With effect from 1 Feb 2013, CPF eSubmission service will no longer be available on Velocity@ocbc. For more information on how you can submit your employees' CPF contribution details and make

Login

User Name

Password

Organisation ID

Login

Learn how to clear your cache

To refresh your cache:

Windows users: Press [CTRL]+[F5]
Mac users: Press [Command]+[R]

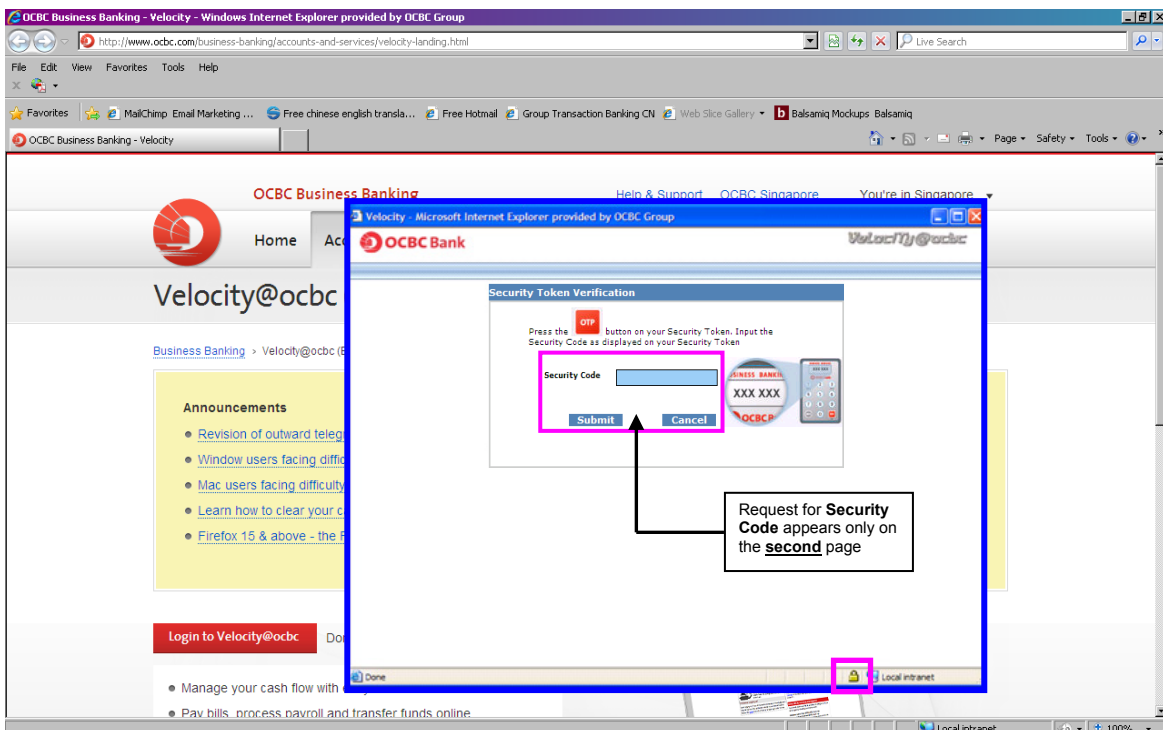
Alternatively, you may learn how to clear your Java and browser cache by following the steps [here](#).

Note: Please do not add this page to your Favorites. To add to Favorites, please use <http://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

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

Security Lock icon to indicate that this is a secured site



OCBC Business Banking - Velocity - Windows Internet Explorer provided by OCBC Group

http://www.ocbc.com/business-banking/accounts-and-services/velocity-landing.html

OCBC Business Banking

Home Account

Velocity@ocbc

Business Banking > Velocity@ocbc

Announcements

- Revision of outward teleg
- Window users facing diffic
- Mac users facing difficulty
- Learn how to clear your c
- Firefox 15 & above - the F

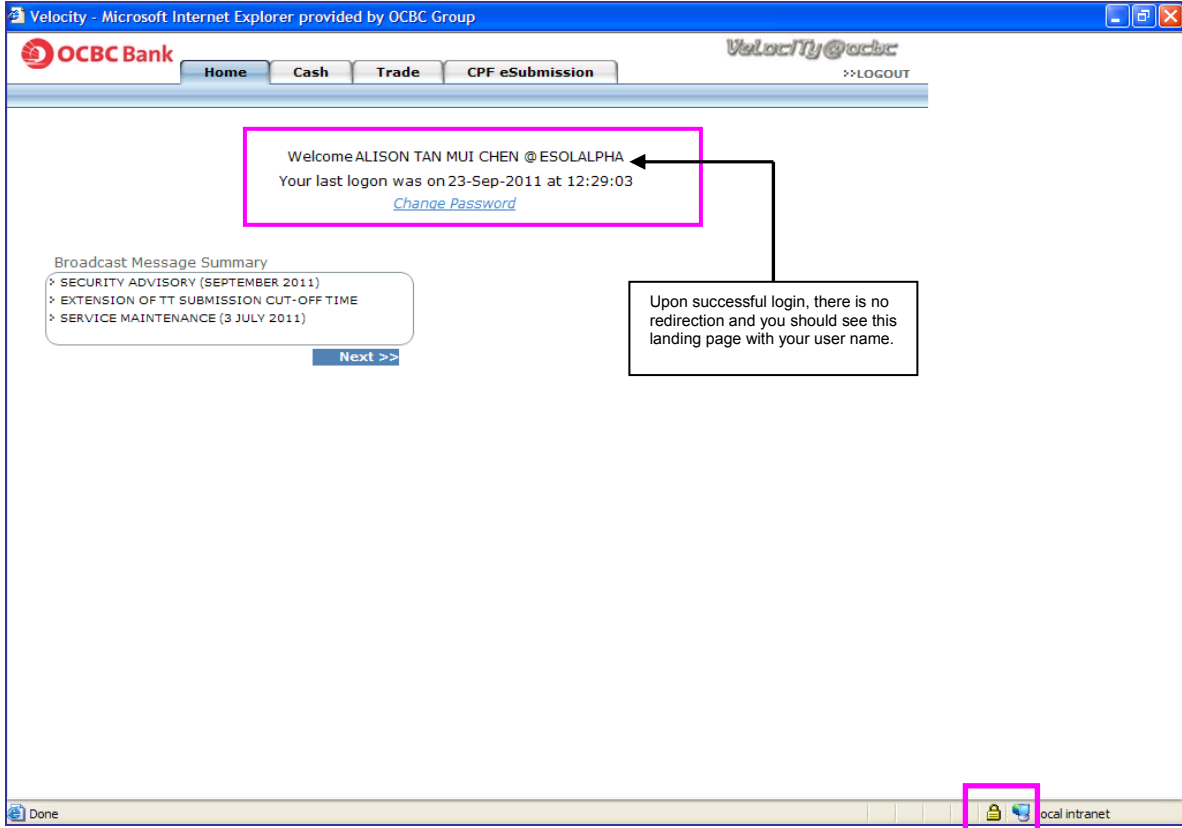
Security Token Verification

Press the **OFF** button on your Security Token. Input the Security Code as displayed on your Security Token

Security Code

Submit Cancel

Request for Security Code appears only on the second page



Velocity - Microsoft Internet Explorer provided by OCBC Group

OCBC Bank **Velocity@ocbc** Home Cash Trade CPF eSubmission >>LOGOUT

Welcome ALISON TAN MUI CHEN @ ESOLALPHA
Your last logon was on 23-Sep-2011 at 12:29:03
[Change Password](#)

Broadcast Message Summary

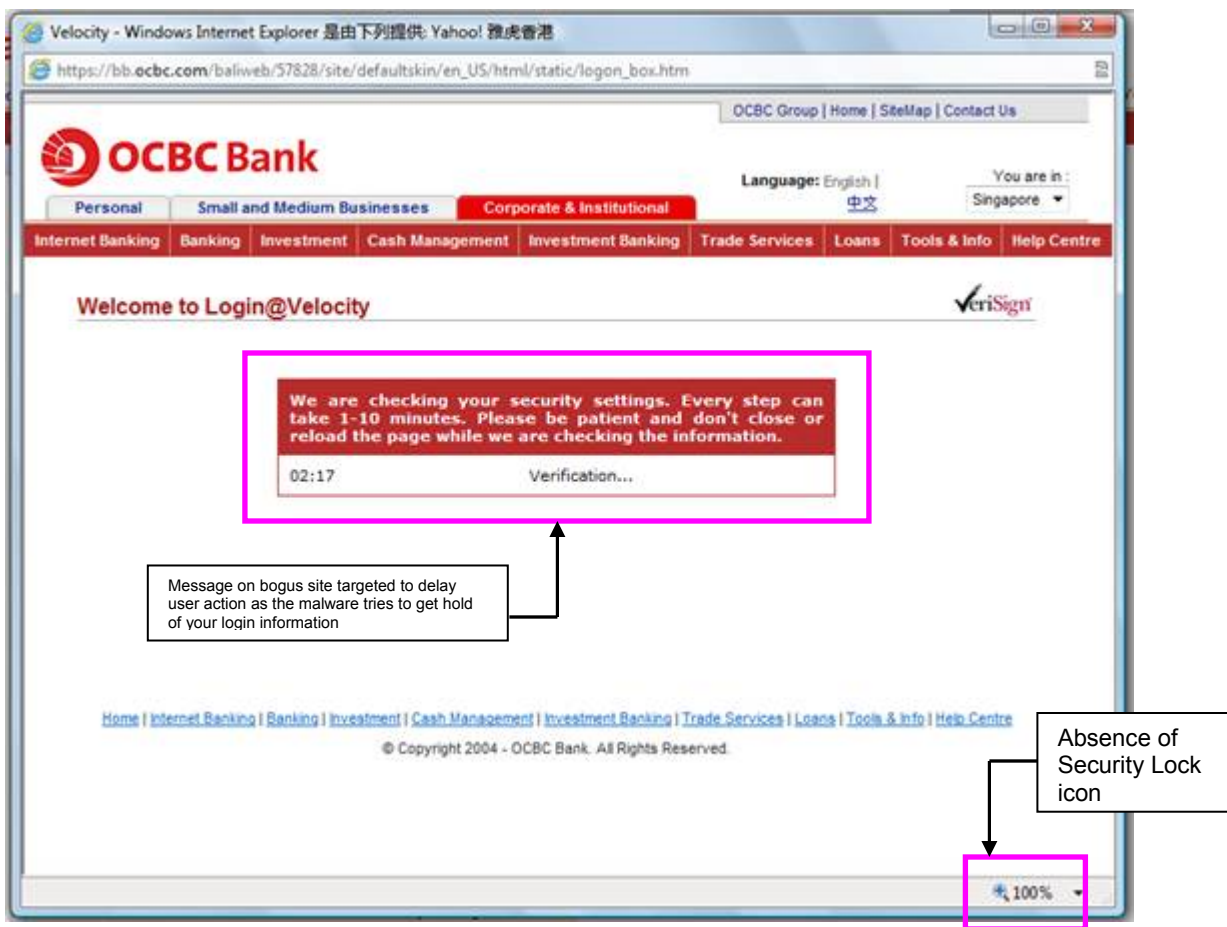
- ✕ SECURITY ADVISORY (SEPTEMBER 2011)
- ✕ EXTENSION OF TT SUBMISSION CUT-OFF TIME
- ✕ SERVICE MAINTENANCE (3 JULY 2011)

[Next >>](#)

Upon successful login, there is no redirection and you should see this landing page with your user name.

Done local intranet

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: Authorisers are advised to call the Bank to reset their password.

For clarification, please contact us at 6538 1111 (or +65 6538 1111 if calling from overseas).