Security Tips On Email

With the Email emerging as an increasingly important communication tool, it is critical to take precautionary measures against cyber frauds.

Be wary of:

- any false e-mail address, logo or graphic designed to mislead you into accepting the validity of any email or website;
- any fake domain name which appears to be the Bank's website or the website of any other financial institution;
- any hyperlink to any fake website;
- any embedded form in any email; or
- or any other technique or method designed to mislead you or trick you into providing personal details, such as your Internet Banking, Phone Banking or ATM PIN, user name or password, or any other sensitive information or downloading a virus

Never access OCBC Internet Banking from a link in an email.

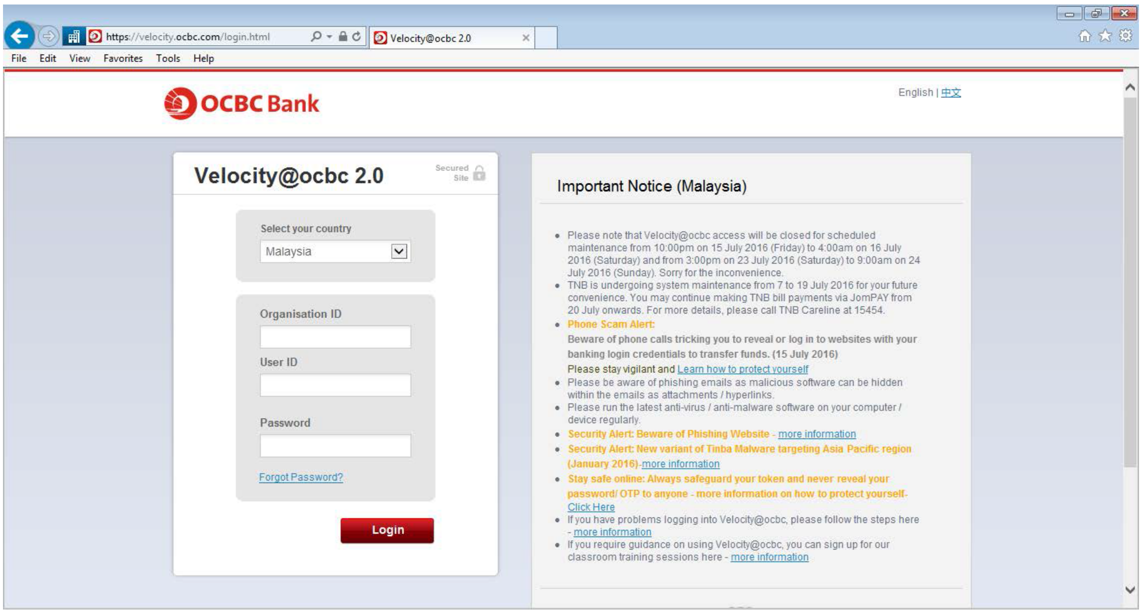
Enter the Domain Name

Always enter the domain name of the Bank (ie. https://velocity.ocbc.com) into your browser when logging onto the Bank's website. You are advised to take the necessary precautions and not to accept any websites at face value that redirects the link to OCBC Bank Group. The exception to Institutions in Malaysia is Bank Negara. If you are in doubt, kindly contact us at 1300-88-7000 (within Malaysia)/ (603) 8317 5200 (outside Malaysia) from Monday to Friday, 9am to 6pm (excluding public holidays).

Be aware of Phishing

Phishing is the term coined by hackers who imitate legitimate companies in e-mails to entice people to share passwords or credit card numbers. Before entering your User Name and Password, you should always ensure that the website you are visiting belongs to OCBC Bank. This can be verified by the URL displayed in your browser as well as the Bank's name in its digital certificate. This precaution will ensure that you are not revealing your OCBC Bank Internet Banking Access Code and PIN to a website other than OCBC Bank. Always check that our website address changes from http:// to https:// and a security icon, usually in the form of a lock or key, appears when authentication and encryption is expected.

The login page for Velocity@ocbc:



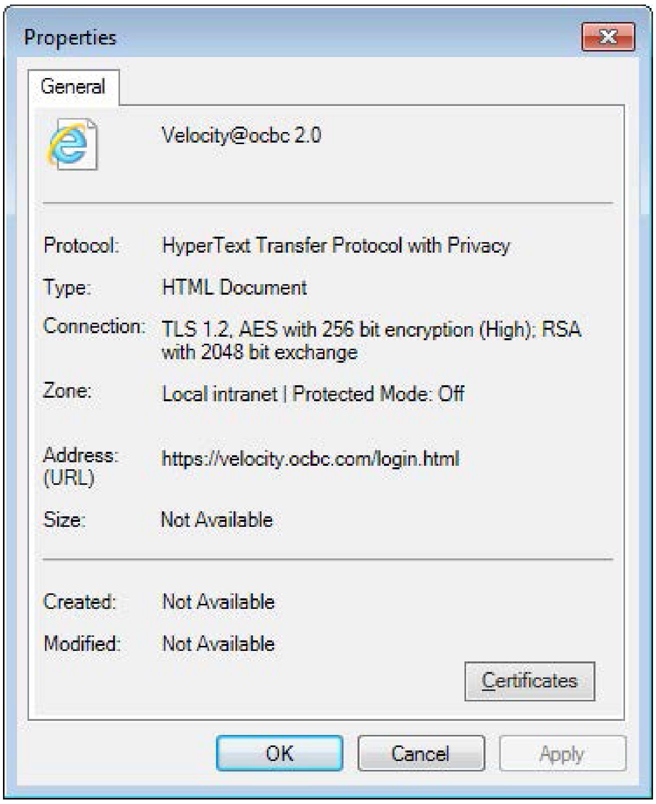
Important Notice (Malaysia)

- Please note that Velocity@ocbc access will be closed for scheduled maintenance from 10:00pm on 15 July 2016 (Friday) to 4:00am on 16 July 2016 (Saturday) and from 3:00pm on 23 July 2016 (Saturday) to 9:00am on 24 July 2016 (Sunday). Sorry for the inconvenience.
- TNB is undergoing system maintenance from 7 to 19 July 2016 for your future convenience. You may continue making TNB bill payments via JomPAY from 20 July onwards. For more details, please call TNB Careline at 15454.
- Phone Scam Alert:

  Beware of phone calls tricking you to reveal or log in to websites with your banking login credentials to transfer funds. (15 July 2016)

  Please stay vigilant and Learn how to protect yourself
- Please be aware of phishing emails as malicious software can be hidden within the emails as attachments / hyperlinks.
- Please run the latest anti-virus / anti-malware software on your computer / device regularly.
- **Security Alert: Beware of Phishing Website** - more information
- **Security Alert: New variant of Tinba Malware targeting Asia Pacific region (January 2016)**-more information
- **Stay safe online: Always safeguard your token and never reveal your password/ OTP to anyone - more information on how to protect yourself-** Click Here
- If you have problems logging into Velocity@ocbc, please follow the steps here - more information
- If you require guidance on using Velocity@ocbc, you can sign up for our classroom training sessions here - more information

Perform a right mouse click on this page and select "Properties". The following window will pop-out.



Velocity@ocbc 2.0

Protocol: HyperText Transfer Protocol with Privacy

Type: HTML Document

Connection: TLS 1.2, AES with 256 bit encryption (High); RSA with 2048 bit exchange

Zone: Local intranet | Protected Mode: Off

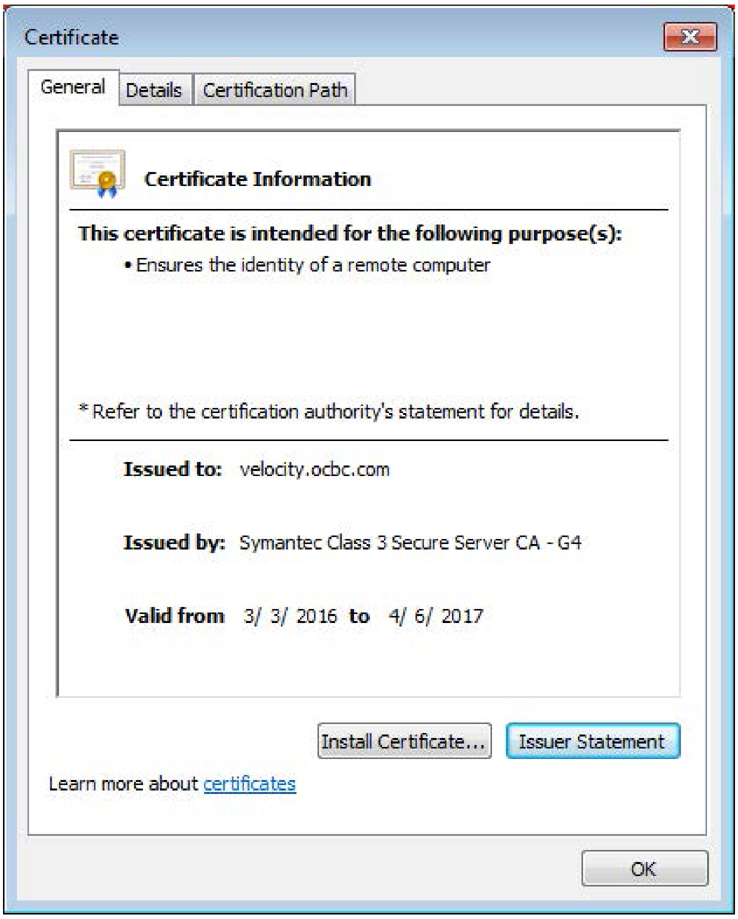
Address: (URL) https://velocity.ocbc.com/login.html

Size: Not Available

Created: Not Available

Modified: Not Available

Click on "Certificates" to display the certificate that ensures the authenticity of the website.



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

* Refer to the certification authority's statement for details.

Issued to: velocity.ocbc.com

Issued by: Symantec Class 3 Secure Server CA - G4

Valid from 3/ 3/ 2016 to 4/ 6/ 2017

Ensure the following on the Certificate:

- The Certificate is issued to velocity.ocbc.com
- The Certificate is issued by Symantec
- The Certificate has a valid date (not expired)

You are encouraged to delete junk mail, chain mail or any other unsolicited email. Do not open email attachments from strangers.

If you discover or believe that there are fraudulent e-mails, fake websites or other scams directed at you or any other customer of the Bank, the Bank or the OCBC Bank Group, please notify the Bank immediately at at 1300-88-7000 (within Malaysia)/ (603) 8317 5200 (outside Malaysia) from Monday to Friday, 9am to 6pm (excluding public holidays).