Phishing alert

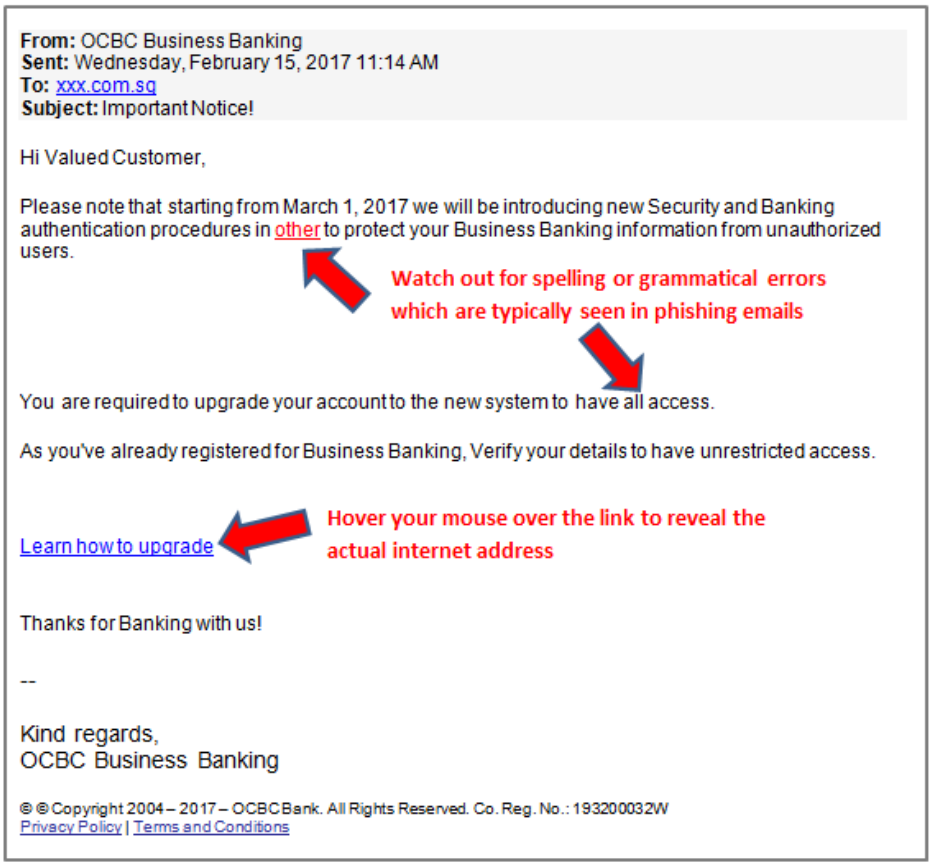
08 March 2017
Threat: **Phishing scam**
Severity: **Medium**

What it does

Phishing emails which contain hyperlink to phishing website that resembles Velocity@ocbc's login page.

The hyperlink in the email will redirect you to a phishing website which then prompts you to enter your login credentials such as your Organisation ID, User ID, Password or One Time Password (OTP). Upon which, fraudulent transfers may be effected from your account(s).

To avoid any unauthorised access to your bank account(s), please be mindful to never enter such information on to links to websites sent via emails. We advise you to stay vigilant and take the necessary precautions to protect yourself. Please see below for a sample of such phishing emails.



How to protect yourself

- Pay attention to the URL of a website. Be aware of malicious websites as they may look identical to a legitimate site, but the URL is different (e.g., ".com" vs ".net"). A legitimate OCBC website will end with ".com" instead of ".net". E.g. Velocity@ocbc login page URL should show as https://velocity.ocbc.com

- Never reveal or key in your banking details such as Organisation ID, User ID, Password or OTP into websites or email soliciting for these types of information.

- Use different passwords, especially for your Velocity@ocbc login and email account, along with any other online accounts (e.g. Subscription-based sites, online merchants, social media, etc).

- Call the bank immediately if you detect any suspicious alerts or transactions not performed by you.

- Always keep your contact details records such as mobile number or email address with the bank up-to-date.

- Always access Velocity@ocbc login page via ocbc.com.my

If you notice any unusual or unauthorised transactions such as receiving SMS transaction alerts or email notifications for transactions you did not initiate, please inform us immediately by calling us at 1300 88 7000 (within Malaysia) or 603-8317 5200 (outside Malaysia).

We would like to assure you that our internet banking websites remain secure. As malicious emails and websites are constantly evolving, we strongly recommend that all users always stay vigilant and verify the authenticity of all outgoing payment instructions, on top of scanning all devices regularly.

At OCBC Bank, protecting your information is our priority. For more about online security and how to protect yourself from fraud, please visit: http://www.ocbc.com.my/business-banking/help-and-support/tips-and-notices.html