Security Alert: New variant of Tinba Malware targeting Asia Pacific region (January 2016)

Dear customers,

We would like to bring your attention to recent reports of a new variant of Tinba financial malware that is targeting the Asia Pacific region, with Malaysia being one of the most frequently targeted country.

Once the machine/device is infected, the malware may inject bogus webpages into the browser that phish for banking credentials. With the stolen credentials, the fraudster then performs financial transactions without the user knowing until it is too late.

We would like to remind you to stay vigilant, exercise caution and adopt good online banking practices:

- Do not provide authorisation for transactions that you did not initiate or request
- Do not open suspicious attachments in emails received, even if they are from senders you know. These attachments may appear in the form of invoices or other accounting documents.

How Tinba Works

1) Your machine/device can be infected by simply clicking on links provided in emails or visiting infected websites.

2) Once infected, an unusual message (like the one shown below) may also be displayed on the victim's machine while fraudulent activity is carried out in the background:

> ***"We are working on updating the database, so that the service is temporarily unavailable. We will try to resume the service as soon as possible. Please try again in a few hours."***

How to avoid becoming a victim

- Ensure your machine/device's **operating system, Internet browsers**[1] **and plugin/extensions are all up-to-date**

- Ensure your machine/device's operating system is **enabled to support Transport Layer Security (TLS) 1.2 and above** under *'**Internet Options**'* > '***Advanced***' *tab* > '***Security***'

- Be on the alert for any irregularities during your internet banking session (e.g. **banking website redirecting to third party website offering hotline number, altered login flow and unsolicited requests for tokens**)

- 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". Eg. Velocity@ocbc login page: https://bbmy.ocbc.com OR https://velocity.ocbc.com

[1] For Internet Explorer, you are advised to use IE11 as Microsoft is no longer providing security patches for IE10 and below.

- Avoid surfing unfamiliar and unsecured websites. An example of an unsecured website URL starts with "http" as opposed to a **secured website URL starting with "https"**. Eg. Velocity@ocbc login page: https://bbmy.ocbc.com OR https://velocity.ocbc.com

- We recommend that you **install and maintain the latest anti-virus software** (eg. McAfee, Norton Anti-virus). Ideally, do also install and maintain anti-malware software (eg. Malwarebytes), firewalls, and email filters. Run these applications on your devices regularly.

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

- Make use of the anti-phishing features offered by your email client and web browser. Information about known phishing attacks is also available online at http://www.antiphishing.org.

- Review your email accounts and make sure emails containing attachments that are confidential in nature are deleted eg. copies of IDs, invoices, scanned forms with signatures, etc. These documents can be saved or archived to your computer hard disk for safekeeping.

- Do not reveal personal or financial information in email and do not respond to email solicitations for these types of information. This includes clicking on links included in emails.

- If you are unsure whether an email request is legitimate, verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information.

- Be alert and watch out for unsolicited phone calls, visits, or email messages from individuals asking about employees or other information about your company. If an unknown individual claims to be from a legitimate organisation, verify his or her identity directly with the organisation. Do not provide any information unless you are certain that the person is authorised to have the information.

What to do if you think your machine/device has been infected

If you suspect that your machine/device has been infected by malicious software while on your internet banking site, **please DO NOT proceed with your online banking activities and follow the steps below:**

1. Cancel any suspicious-looking transactions in Velocity@ocbc.
2. Close the browser.
3. Ensure that your anti-virus/anti-malware software is up to date.
4. Run your anti-virus/anti-malware software and scan the files on all devices (eg. laptops, desktops) that you use to access online banking. If your computer is not installed with an anti-virus software or anti-malware, please install the latest version immediately and perform a scan on your devices.
5. Change your password for Velocity@ocbc on a different device/PC immediately.
6. After the infected computer has been scanned and clean, restart and login to Velocity@ocbc. You should not encounter the same bogus site again upon login if the malicious software has been completely removed.

7. If you suspect that the malicious software has not been successfully removed, please do not use the same computer for any online banking transactions and seek professional help to remove the malicious software. Remember to run an anti-virus/anti-malware scan on an alternative computer to make sure it is uninfected before performing any online banking transaction.

We would like to assure you that our internet banking websites remain secure. As malicious software are constantly evolving, we strongly recommend that payment makers and authorisers 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?

If you have any further queries, please contact us from 8:30am to 6:00pm (Monday to Friday, excluding public holidays) at 1300 88 7000 (within Malaysia) or 603-8317 5200 (outside Malaysia).