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

安全警示: Tinba恶意软件的新变种正瞄准亚太地区

Dear customers,
尊敬的客户：

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
我行在此呈请您注意最近关于Tinba金融的恶意软件新变种正瞄准亚太地区的报告。

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.
一旦机器/设备被感染，此恶意软件将向浏览器中注入伪造的网页，以钓取银行的证书。 通过盗取的证书， 骗子可以在用户不知晓的情况下进行金融交易,，等用户发觉时已经太晚了.

We would like to remind you to stay vigilant, exercise caution and adopt good online banking practices:
我们在此提醒您保持警惕, 谨慎操作并采用良好的网上银行操作实践：

- Do not provide authorisation for transactions that you did not initiate or request
  不要对不是您发起的或者要求的交易进行授权
- 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.
  不要打开收到邮件中的可疑附件， 即使邮件是由您认识的人发送给您的。因为可疑附件也可能伪装成发票或者其他会计文件的形式。

How Tinba Works
恶意软件如何工作

1) Your machine/device can be infected by simply clicking on links provided in emails or visiting infected websites.
   您的机器/设备会因为简单点击邮件中的链接或者访问别感染的网站而被感染。
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:
   一旦被感染, 一个不常见的信息(例如下面显示的内容)可能在被害人的机器上显示,同时欺诈活动在背后进行。

> ***"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."***

我们正在进行数据的升级， 所以暂时不能提供服务。 我们将尽快恢复服务。 请在几小时后再次尝试。

How to avoid becoming a victim
如何避免变成受害人

- Ensure your machine/device's **operating system, Internet browsers[1] and plugin/extensions are all up-to-date**
  确保您的机器/设备的操作系统, 互联网浏览器[1]和插件/扩展件都及时更新。

[1] *For Internet Explorer, you are advised to use IE11 as Microsoft is no longer providing security patches for IE10 and below.*
对于互联网浏览器,建议您使用IE11, 因为Microsoft已不再为IE10及以下版本提供安全补丁

- 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*'
  确保您的机器/设备的操作系统能够支持传输层安全(TLS)1.2及以上版本, 在"互联网选项>高级项目>安全 中确认。

- 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**)
  对于您网上银行使用中的任何异常情况保持警惕(例如: 银行网站转向提供热线号码的第三方网站, 登录流程改变和未经提出的令牌要求)。

- 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 WING HANG website will end with ".com" instead of ".net". Eg. Velocity@ocbc login page: **https://cbcn.ocbc.com/corporbank/**
  注意一个网站的链接.请注意恶意网站即使表面上和真实的网站看上去一样,但URL是不同的.(例如."com" 对比 "net"). 一个真实的华侨永亨银行网站将使用".com"结尾,而不是".net".例如. Velocity@ocbc 的登录链接: https://cbcn.ocbc.com/corporbank/

- 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://cbcn.ocbc.com/corporbank/**
  防止浏览不熟悉和不安全的网站. 例如一个不安全的网站链接起始是"http", 相反一个安全网站的链接起始是"https". 例如: Velocity@ocbc登录链接是: https://cbcn.ocbc.com/corporbank/

- 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.我们推荐您安装并维护最新的反病毒软件 (例如: McAfee, Norton Anti-virus). 在理想情况下,也同时安装和维护反恶意软件 (例如: Malwarebytes), 防火墙和邮件过滤器. 定期在您的设备上运行这个应用程序.

- 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]
  使用不同的密码, 特别对您Velocity@ocbc 的登录和邮箱账户密码, 设置与其他网上账户不同的密码. [例如: 订阅基础的网站, 网上商户, 社会媒体等等]

- 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.
  使用您的邮箱客户段和网络浏览器提供的反钓鱼功能, 关于钓鱼攻击的相关信息和知识可以在http://www.antiphishing.org上获得.

- 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.检查您的邮箱账户并确保带有保密附件的邮件都被删除. 例如: ID的副本, 发票, 带有签字样本的扫描件等.这些文件可以保持或者归档在您电脑的硬盘中已安全保管.

- 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.不要将个人或者财务信息在邮件中揭示,不要恢复要求提供此类信息的邮件. 这也把包括邮件中提供的链接.

- 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.
  如果您不能确认一个邮件请求是否真实时, 请直接联系公司进行确认. 不要使用网站上提供的相关联系方式, 检查以前的对帐单并使用其提供的联系方式.

- 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.
  请警惕和小心非请求的个人要求提供雇员或您公司其他信息的的电话,拜访或者邮件信息。如果一个不认识的个人声称来自一个真实组织,。直接和此组织核实他/她的身份，不要提供任何信息除非您可以确认此人已被授权获得此信息。

What to do if you think your machine/device has been infected
如果您觉得您的机器/设备已经被感染后如何处理

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:**
如果您在网上银行网站上怀疑您的机器/设备已经被恶意软件感染, 请不要进行任何网上银行活动并按照以下步骤操作:

1. Cancel any suspicious-looking transactions in Velocity@ocbc.
   在Velocity@ocbc上取消任何有可疑的交易。
2. Close the browser.
   关闭浏览器
3. Ensure that your anti-virus/anti-malware software is up to date.
   确保您的反病毒/反恶意软件程序已及时更新
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.
   运行您的反病毒/反恶意软件程序并扫描您用来访问网上银行的所有设备内的文件.(例如:笔记本,台式机) 如果您的电脑没有安装一个反病毒/反恶意软件程序,请立即安装最新版本的程序并对您的设备进行一次扫描。
5. Change your password for Velocity@ocbc on a different device/PC immediately.
   立即使用不同的设备/个人电脑修改您Velocity@ocbc的密码
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.
   在被感染的电脑被扫描和清理后,重启并登录Velocity@ocbc. 如果恶意软件已经被完全清除,则您登录后不会遭遇同样的伪造网站.
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.
   如果您怀疑恶意软件没有被完全清除, 请不要使用此电脑操作任何网上银行交易并寻求专用人员的帮助以清除恶意软件. 请记住在使用其他电脑操作任何网上银行交易前,运行反病毒/反恶意软件程序进行扫描以确保此电脑未被感染.

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.

我行向您保证我行的网上银行网站是安全的. 鉴于恶意软件也在持续进化, 我行强烈建议所有付款指示的制作人和授权人在定期扫描所有设备的基础上, 时刻保持警觉并核查所有对外付款指示是否有效授权.

At OCBC WING HANG Bank, protecting your information is our priority. For more about online security and how to protect yourself from fraud, please visit: www.ocbc.com.cn对于华侨永亨银行, 保护您信息的安全是我们的首要任务. 如您想了解更多网上银行安全及如何保护您远离欺诈, 请浏览 www.ocbc.com.cn

If you have any further queries, please contact us from 9:00am to 6:00pm (Monday to Friday, excluding public holidays) at 40089 40089

如您有更多疑问,请在上午9点至下午6点拨打 40089 40089 联系我行(周一至周五,节假日除外)。

Co.Reg.No:193200032W