| Eurograbber virus WARNING|

Eurograbber Virus is a group of variants of Zeus that include Spyeye, CarBerp and ZitMo. This virus breaks the two-factor authentication security method, one of the methods that are being widely used by the banks thanks to its high reliability.

The scam of using Eurograbber to steal money from bank happens as follows:

(1) Hackers use trickery to make customers access a dangerous link with virus Eurograbber, the virus breaks into computers of customer and display fraudulent notification from banks to trick customers to supply **customers' telephone number**.

(2) After having telephone number from the customers, hackers continue to **counterfeit message** from banks to request setting account control software. In fact, it is the counterfeited malware that is used to steal authentication message from banks.

(3) By obtaining login information, account number and password, hackers can withdraw money at banks without any knowledge from customers.

Currently, there is no case recorded in Vietnam; but to protect the Bank's customers, we request customers to note the following points as using Online banking on customers' computer and mobile phone:

- Check that your antivirus software is up to date.
- Ensure that the SMS messages reflect your Online Banking transaction requests. For example, if you receive an SMS message for a beneficiary addition or funds transfer that contains an account number that you do not know, do NOT enter it into the Online Banking and inform the Bank immediately.
- SMS Message sent from Standard Chartered bank is always from: +8069; 1900545406; Stanchart.
- Check the content of SMS carefully, if customers find any suspicious; please immediately contact the bank.
- For your security, do not click on links from emails, install any programs from doubtful origins or perform online transactions on computers that you suspect are compromised.
- Always access our Online Banking service by typing in the correct URL **(http://www.standardchartered.com.vn).**
- Read other security tips.

Important NOTE

The **Bank will never ask** for your **Phone number** via online banking or email or over the phone or via SMS. And the **Bank will never ask** for your log **in password** via email or phone or SMS. If you suspect that your computer or your bank accounts have been compromised while banking online with us, please contact us immediately.

Bank's contact: 84-8-3911 0000 or 84-4-3696 0000
Address:

- 1st Floor, Saigon Trade Center; 37 Ton Duc Thang, District 1, HCM city.
- Ground Floor, CDC Building, 25 Le Dai Hanh, Hai Ba Trung district, Ha Noi
- Ground Floor, Hanoi Towers, 49 Hai Ba Trung, Hoan Kiem district, Ha Noi.