Press Release (Immediate Release)   19 May 2015

Dah Sing Bank Security Alert on e-Banking / i-Securities Service

Dah Sing Bank, Limited ("DSB") has discovered a malware that may affect users of DSB e-Banking / i-Securities service. This malware may spread through phishing emails with malicious attachment. When the said malicious attachment is opened, the malware infects the customers' computers and a pop-up screen requesting customers to provide personal information will appear. Once customers' computers are infected, the malware will attempt to steal the customers' credentials such as credit card number, expiry date, CVC2, credit limit and date of birth by prompting a new screen requesting for such credentials during logon of e-Banking / i-Securities.

DSB would like to advise that the above pop-up screen has no affiliation or connection whatsoever with DSB and / or the Dah Sing Financial Holdings Limited, nor any of its subsidiaries. DSB would not ask customers to provide credentials through pop-up screens when they log in to or when they are using their e-Banking / i-Securities accounts. If customers encounter the above issue or suspect that the computer in use has been infected, customers may consider taking the following actions:

- Do not input any information to any unusual pop-up screen
- Do not log in or proceed with any transactions on e-Banking / i-Securities services until the computer is disinfected
- Install antivirus software and make sure the virus definition file is up-to-date
- Scan and clean up your computer with the antivirus software before trying to log in e-Banking / i-Securities again

DSB has reported the case to the Hong Kong Monetary Authority and the Hong Kong Police. If customers suspect that their computers have been infected and credentials have been captured, please call the Security Incident Hotline at 3101 3111.

~ The End ~