



Re: Phishing E-mail Alert

Dear SCB Business Net Customer,

It has come to our attention that some SCB customers have received phishing e-mails advising fake fund transfer details and status reports for domestic and cross-border remittances as well as containing document file attachment. These e-mails are sent in an attempt to lure recipients to click the attached file to obtain sensitive personal information. The disclosed sensitive personal information will be used for conducting online transactions and activities such as online shopping, applying for credit cards, committing illegal activities, and other offenses.

SCB has quickly responded to this fraud by working with all concerning segments to prevent potential damage and implement effective measures to control the situation. At the same time, customers are kindly requested to take caution when receiving e-mail messages from unrecognized senders, and to always stay alert for e-mail messages with suspicious content from illegitimate sources. SCB would like to provide some useful tips and recommendations for verifying e-mail messages, as follows:

1. Look out for e-mail content that appears differently from that regularly received from SCB, or e-mail messages from senders who have never contacted you before.
2. Transactions mentioned in the e-mail did not occur.
3. Do not click any attached file before carefully verification.
4. If you have any questions, please directly contact your Relationship Manager or call 02-722-2222.

SCB would like to request that all customers exercise extreme caution for this type of fraud in order to prevent any potential damage to yourself or trade partners.

Yours Sincerely,
Siam Commercial Bank PCL