親愛的客戶:

隨著金融機構報告的網絡釣魚攻擊越來越多，我們強烈敦促大家保持警惕，防止網絡釣魚詐騙偽裝成銀行或政府機構等可信賴的機構，企圖獲取個人信息、密碼或信用卡詳細信息。

1/ 為了保護您的隱私並防止可能的損失，對於惡意攻擊者發送包含透過電子郵件作為入侵系統的一種手段，所謂宏指令的文件 (文件名如: xls, xlsb, xlsm) ，應有所警惕。攻擊模式描述如下：

(a) 寄件者多為偽冒成業務往來或內部員工之姓名(實際寄件者非當事人)。

(b) 郵件主旨多為回覆 (Re : )或轉寄(Fw：)開頭之信件。

(c) 郵件夾帶含有巨集指令之Excel附加檔案(如附檔名為 xls、xlsb、xlsm之文件檔)。

如果您不小心打開了附件並啟用了”宏”，它會執行宏指令來下載惡意程序。

2/ 請您在使用電子郵箱時請遵守以下安全注意事項:

- 注意郵件主旨與寄件者是否與本身相關，不開啟與本身無關之電子郵件。
- 注意內含附件之郵件，不開啟與業務無關之檔案。
- 注意內含其他網站連結之郵件，不連結及登入未經確認的網站。
- 即便與業務往來相關的寄件者或網站連結，也應仔細驗證寄件者EMAIL或網站URL正確性，避免被高度相似字元混淆(如數字0與字母O、數字6與字母b..等)。

如果您收到可疑的通訊，請不要透露您的個人或賬戶信息，並立即致電銀行作業主管熱線 (65)6771-5111 分機：333 進行核實。

如果您在可疑通信中提供了個人或賬戶信息或進行了任何金融交易，請聯繫銀行作業主管熱線 (65)6771-5111 分機：333 。