UOB 大華銀行

再仔細看一眼！警覺釣魚簡訊，小心偽冒網址

Phishing SMS messages and fake URLs alert

親愛的客戶您好

近期在台灣發現有詐騙集團假冒銀行名義發送釣魚簡訊至客戶手機，要求點選簡訊上的假網址，藉以收集客戶在網路/電子銀行的認證資料。

為保障您業務安全，請注意本行大華銀行台北分行**不會**發送簡訊來要求您點選簡訊上的網址，並輸入帳號 ID、密碼、或其他用戶身分認證資料。在本行官方網站以外的其他網頁，請**絕對不要**輸入上述的認證資料。

若收到假借本行名義或來路不明之簡訊或郵件，請勿點選連結，並聯繫 165 反詐騙諮詢專線或本行客服專線 (https://www.uobgroup.com/tw/contact-us/index.page)。

Dear customer

Recently in Taiwan, a fraudulent group/cybercriminals sent phishing SMS/text messages to customers' mobile phones under the name of a bank. The message requested for customers to click on the fake URL in the SMS/text message to collect the customer's Internet/e-banking authentication information.

Please note that UOB Taipei Branch will not send SMS/text messages to request for your authentication information. If you receive such SMS/text messages, please do not click on the URL and enter your account ID, password, or other user identification information. Please **never enter** these authentication information on any other web pages other than UOB Taipei Branch official website(s).

Should you receive any SMS/text messages or emails under the guise of our bank or from an unknown source, please do not click on the link and call 165 anti-fraud consultation hotline or UOB Taipei customer service (https://www.uobgroup.com/tw/contact-us/index.page) immediately. (https://www.uobgroup.com/tw/contact-us/index.page).