警告：切勿侵犯版權

閣下將瀏覽的文章/內容/資料的版權持有者為消費者委員會。除作個人非商業用途外， 閣下不得以任何形式傳送、轉載、複製或使用該文章/內容/資料，如有侵犯版權，消費者委員會必定嚴加追究法律責任，索償一切損失及法律費用。

《消費者委員會條例》第二十條第(1)款其中有規定，任何人未經委員會以書面同意，不得發布或安排發布任何廣告，以明示或默示的方式提述委員會、委員會的刊物、委員會或委員會委任他人進行的測試或調查的結果，藉以宣傳或貶損任何貨品、服務或不動產，或推廣任何人的形象。有關該條文的詳情，請參閱該條例。

本會試驗的產品樣本由本會指定的購物員，以一般消費者身份在市面上購買，根據實驗室試驗結果作分析評論及撰寫報告，有需要時加上特別安排試用者的意見和專業人士的評論。對某牌子產品的評論，除特別註明外，乃指經試驗的樣本，而並非指該牌子所有同型號或不同型號的產品，也非泛指該牌子的所有其他產品。

本會的產品比較試驗，並不測試該類產品的每一牌子或同牌子每一型號的產品。

本會的測試計劃由本會的研究及試驗小組委員會決定，歡迎消費者提供意見，但恕不能應外界要求為其產品作特別的測試，或刊登其他非經本會測試的產品資料。

網上銀行服務越見普及，過往需親身到銀行櫃枱辦理的服務，現在大多可透過互聯網處理，但欺詐網站、「釣魚」網站、偽冒電郵等騙案卻不時發生。根據香港金融管理局的資料，今年首四個月已發現8個欺詐銀行網站，4間銀行被偽冒，情況令人關注。用戶稍一不慎，在欺詐網站輸入戶口資料，便會被盜取登入名稱和密碼等資料，有機會被轉走存款或被利用作不法交易。為免成為受害者，消費者透過電腦或智能電話使用網上銀行服務時，應注意以下提示。

提防誤入欺詐銀行網站被轉走存款

小心保管個人資料

消費者不時收到與銀行服務相關的信件或電郵，當中可能附有個人資料，例如姓名、地址、網上帳戶登入名稱、臨時密碼等。此類資料必須小心保存，若棄置的話，須將印有的敏感資料銷毀，以減低資料外洩的風險。

切勿開啟不明來歷電郵的超連結或附件及流動應用程式

若消費者需要使用網上銀行服務，不應直接點擊從網上搜尋器或電郵得來的超連結，應登入銀行發出的文件或通知內註明的網址，減少被連結至「釣魚」網站的機會，並以瀏覽器的書籤記下網址方便日後使用。部分偽冒電郵及網站以至流動應用程式的偽裝手法高超，一般消費者未必能輕易分辨真假。

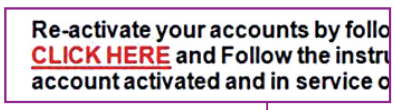
消費者可瀏覽香港金融管理局（金管局）的網頁來確定某銀行是否為認可機構並受金管局監管其在香港經營接受存款及銀行業務；若消費者對銀行網址及流動應用程式存疑，可聯絡金管局及相關銀行。

何謂「釣魚」網站？

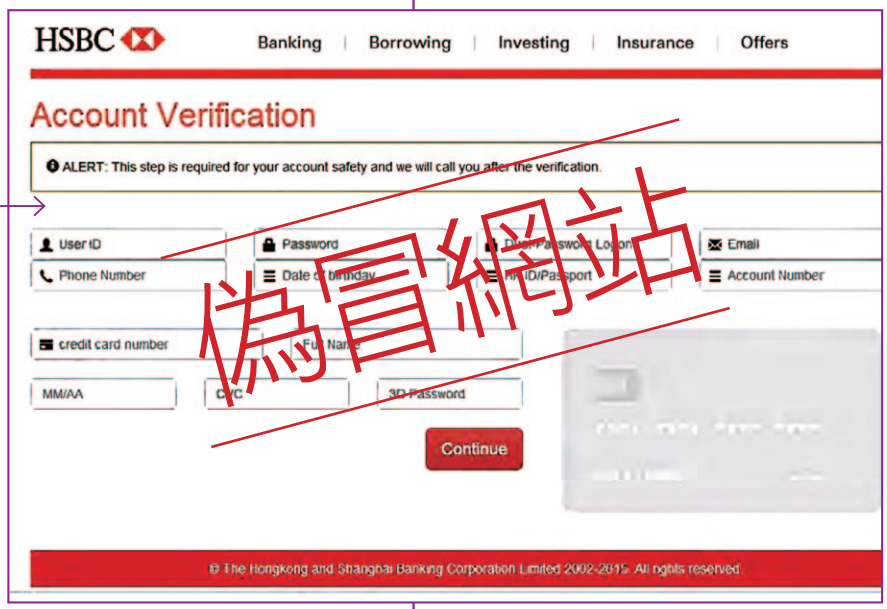
網路釣魚（phishing）指騙徒透過電郵附件及即時通訊的訊息散播惡意程式，或利用超連結將用戶連結至偽冒的銀行網站。當用戶開啟附件或被餌誘到偽冒網站登入帳戶時便會上釣，個人及帳戶資料會被「釣」走。

使用雙重認證

由於雙重認證需要用戶提供額外認證資料來核實身份，即使不法之徒已成功登入用戶的網上銀行戶口，若在確認交易



欺詐電郵



資料來源：滙豐銀行於 2015 年 12 月 7 日發出的新聞稿《滙豐就欺詐電郵及偽冒網站發表聲明》。

雙重認證知多點

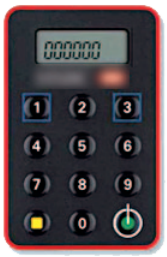
雙重認證指利用兩項不同性質的資料來核實網上銀行客戶的身份及權限的保安措施。用戶除了在登入網上銀行戶口時需要輸入一個密碼外，當使用某些理財服務時，需要進行額外認證，例如另外輸入一個一次性密碼（one-time password，OTP）以確認交易。這個一次性密碼通常由銀行以手機短訊形式通知用戶，或經由銀行提供的保安顯示器發出。各間銀行的雙重認證程序各有不同，消費者宜聯絡開戶銀行瞭解詳情。

銀行以手機短訊發放的一次性密碼。

時欠缺所需的額外認證資料，相關交易便無法完成，減低用戶可能蒙受的損失。

受騙個案

有一網上銀行用戶不知道其戶口名稱、密碼及聯絡資料已被盜取，其後，用戶透過手提電話收到銀行發出的一次性密碼，並接到一名訛稱為銀行職員的來電，用戶不虞有詐，向來電者透露了一次性密碼，及後才發現戶口存款已被轉走。為免成為下一名受害者，消費者必須小心保管網上銀行戶口的登入名稱、密碼，以及保安顯示器，絕對不可向其他人透露銀行發出的一次性密碼。



其中一款保安顯示器

勿透過 Wi-Fi 熱點作網上銀行交易

要加強保安，消費者可使用安裝了防火牆、設有網絡釣魚防護功能的防毒及防間碟軟件的私人電腦或智能電話，應盡量避免使用公眾電腦或透過不明電腦網絡（包括Wi-Fi熱點）來登入私人帳戶或進行網上銀行交易。公眾電腦及網絡的目的是方便市民大眾作一般網頁瀏覽或查詢，未必會安裝適當的保安軟件。近年亦發現有黑客利用Wi-Fi熱點進行攻擊，特意設立與知名機構的Wi-Fi熱點名稱相近的「釣魚Wi-Fi」網絡來吸引用戶使用。若消費者使用防衛能力較弱的裝置或網絡進行網上理財，或會令網絡騙徒有機可乘，在不知情下被盜取敏感資料。

時刻小心 保持警惕

消費者應謹記本港的銀行絕不會向客戶發出附有接駁至交易網站的超連結的電郵，亦絕不會以電郵、電話或親身要求客戶提供各種登入網上銀行戶口及確認交易的敏感資料（包括戶口的登入名稱、登入密碼及一次性密碼）。若消費者從任何渠道收到自稱銀行職員查詢及要求提供敏感資料，應斷然拒絕並立即致電有關銀行的熱線電話核實來電者的身份，不要單憑來電顯示去辨別。消費者可於金管局、香港銀行公會或相關銀行網站查閱熱線號碼和相關資訊。

消費者亦可參考金管局網站所提供的網上銀行保安資料：

- 認可機構及本地代表辦事處紀錄冊：http://vpr.hkma.gov.hk/cgi-bin/vpr/index.pl?lang=chi
- 欺詐銀行網站、偽冒電郵及類似的詐騙事件：http://www.hkma.gov.hk/chi/other-information/fraudulent-bank-websites.shtml
- 網上銀行－雙重認證：http://www.hkma.gov.hk/chi/key-functions/banking-stability/internet-banking/two-factor-authentication.shtml
- 使用網上銀行的主要保安提示：http://www.hkma.gov.hk/chi/key-functions/banking-stability/consumer-corner/strengthening-financial-consumer-protection/consumer-education-programme/internet-banking.shtml