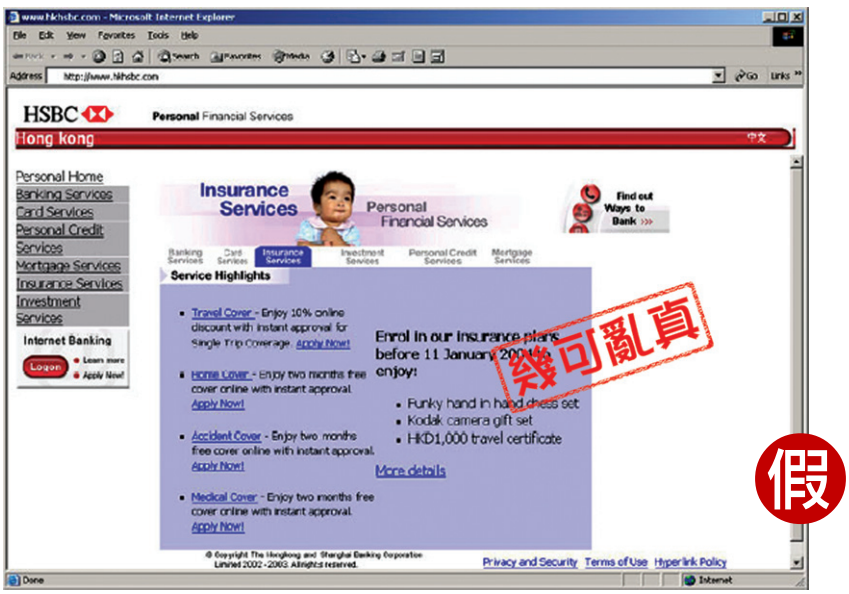
假銀行網站日益猖獗 教你自保招數

自2003年6月出現多個假銀行網站，有些像真度極高，消費者一不留神隨時誤墮陷阱。雖然警方和銀行均指出暫時並未有消費者損失金錢，但假網站可能會影響公眾對電子銀行的信心。銀行應採取更有效的預防措施，加強網上保安，保障客戶的財產；而消費者亦要積極自強，多瞭解個人資料保密的知識，防範被騙。



一、網上欺騙手法層出不窮

銀行近年積極推動電子銀行，提供24小時個人服務，減少市民在分行排隊輪候，網上理財乃大勢所趨。高科技為生活帶來方便，但網上欺詐行為令人關注。近期本港發生多宗涉及虛假電郵或網站的騙案，騙徒利用虛假電郵或網站意圖取得銀行客戶的敏感資料。

1. 虛假電郵（fake emails）

騙徒假冒銀行向銀行客戶發放電子郵件，引導客戶按入附於電郵內的「超連結」

辨別真假網址有辦法

騙徒手法層出不窮，消費者要防範被騙，要學懂如何辨別網址真偽。

1. 如何核實網站名稱是否真確?

只有受《銀行業條例》規管的認可機構，才可在香港經營銀行業務或接受存款業務。截至2003年10月，本港有35家銀行提供網上銀行服務。**在香港有提供網上銀行服務的銀行，並非所有域名也是以com.hk收尾，例如：恒生銀行的正式網址是www.hangseng.com，永亨銀行www.whbhk.com，東亞銀行是www.hkbea.com，它們都不是以.hk收尾。**消費者在找尋銀行網址時，要多加留意。

現時申請以.com.hk收尾為域名的公司須要提交證明文件，核實公司是否在香港註冊，要求較以.com收尾的域名嚴謹。有不法騙徒以.com註冊後便在域名內加上hk字眼或以近似真網址的域名魚目混珠，企圖令消費者誤墮陷阱。最近的例子有：www.hkhsbc.com (假)，www.hsbc.com.hk (真)。

消費者可在金融管理局網站(www.hkma.gov.hk)的「消費者資訊」一欄內查閱認可機構名單，或致電2878 8222查詢。為方便消費者核實連接的網站是銀行的正式網站，本會建議金管局考慮在認可機構名單內加入網址資料。此外，消費者亦可在香港銀行公會的網站(www.hkab.org.hk)的「會員」一欄查閱銀行的正式網址。

2. 有無「安全鎖」?

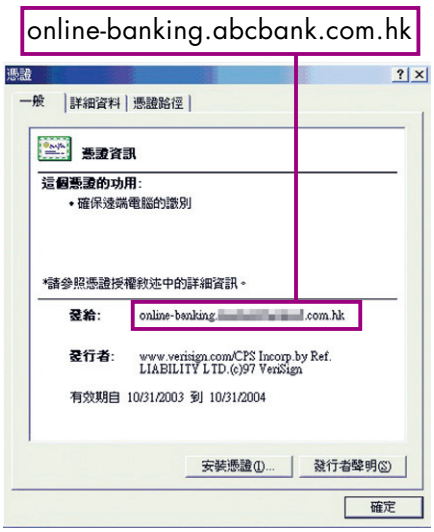
網頁瀏覽器下方顯示的一個小扣鎖或鑰匙，表示傳送到該網站的資料會受到加密技術保護。

使用Internet Explorer登入網上銀行後，留意熒幕右下角顯示一個「安全鎖」標記。

「安全鎖」是網絡加密保安的技術，在用戶端與伺服器之間進行加密與解密，是保障資料安全傳遞的安全編碼系統。「安全鎖」乃由一組數字組成，其安全程度取決於數字的長度，數字愈多，組合便愈多，因而亦愈難被破解，因此，128位元的「安全鎖」，其保安程度便會較64位元的為高。

3. 檢視數碼證書

即使看到「安全鎖」，亦不等於安全。消費者應以滑鼠連按兩次這標誌，網頁會「彈」出安全憑證資訊，詳列出銀行網址、保安核實證明及有效日期，查閱網站的數碼證書確實無誤，才可放心使用網上理財。**偽冒的網站即使可以複製銀行的設計圖像及類似的網站地址，但不可能具有該數碼證書，消費者可依據此辨識網址真偽。**



Internet Explorer安全憑證的熒幕顯示

Internet Explorer「安全鎖」標記

4. 使用電子證書

「電子證書」是香港郵政核證機構發出的認可數碼證書，內載申請人的個人資料及香港郵政編配的專用登記人參考編號。電子證書是外加的保護網屬自動確認模式，毋須藉着鍵盤輸入方式確認，換句話說，即使用戶密碼及資料被竊或電腦被裝上監視軟件，只要騙徒取不到最關鍵的「私人匙」(private key)，亦不能登入客戶的帳戶。當然，消費者要收好「私人匙」，以防外洩。

除香港郵政所發的電子證書外，現時也有銀行接收貿易通Digi-sign的電子證書，及有部份銀行自行發出用戶證書予網上銀行商務客戶。

Netscape Navigator用戶查閱安全憑證

檢查方法：按入功能表上的「安全」，於「安全」資訊網頁中，按「檢視認證」，檢查熒幕有否顯示安全憑證資料

網上銀行安全貼士 TIPS

1.小心選擇及使用網上銀行服務

● 進行網上交易前，要清楚交易對方身份，確保進入真確的網站

○ 審閱所連接的銀行網址的安全憑證是否屬實及仍在有效期內

○ 按銀行文件或單張上列印出來的網址登入，記入瀏覽器上的書簽（如「我的最愛」），以後按此進入

○ 切勿通過附載於電郵內的「超連結」（hyper link）登入網上銀行的網站

○ 切勿以「搜尋器」（search engine）找尋銀行網址，避免連結到假網站

● 瞭解銀行對客戶的保障是否充足，例如：是否已配備完善的保安系統及措施，以及告知客戶對損失的責任

● 不時瀏覽銀行提供的保安提示

● 設置密碼以保護個人電腦免被他人使用

● 設定熒幕保護密碼，避免暫時離開電腦時，有人會趁機偷盜電腦資料

● 於使用銀行網上理財服務時，勿同時開啟視窗進入另一個網址

● 於每次登入銀行網上理財時，核對上一次登入的日期及時間。如發現不正確的資料，應即時通知銀行作處理

● 切勿在公眾或共用電腦使用網上銀行服務，因為對方可能會在電腦上裝設監視軟件

● 安裝防火牆軟件及防電腦病毒軟件，並定期下載防毒軟件的更新檔案，以阻止黑客及電腦病毒入侵

● 使用電子證書，以防被監視軟件記錄資料

● 用畢網上銀行服務，應登出及中斷連線才離開

2. 審慎處理個人資料

● 定期更改網上理財戶口密碼

● 戶口密碼不應選擇容易被猜中的號碼或字母組合，如姓名、出生日期等

● 切勿在不同的網上服務（如銀行網上服務、電子郵件或互聯網服務），使用相同的用戶名稱及密碼

● 小心收藏用戶號碼及密碼，並切勿向任何人(包括銀行職員及警方)，或在網上隨便透露個人資料

● 妥善處理與銀行帳戶有關的文件，如撕毀後丟掉

● 在提供個人資料給網站前，先查閱網站的私隱政策聲明及安全防護措施聲明

● 切勿把戶口資料（如用戶名稱及密碼）記存於瀏覽器，取消瀏覽器的「自動完成/設定」功能，以避免當只輸入過一次的用戶名稱及密碼，下一次再登錄時，電腦就會自動完成登入

○ 移除電腦中「自動設定」功能

在Internet Explorer瀏覽器中取消「自動完成」功能，按一下「工具」清單，按一下「Internet選項」，按一下「內容」定位點，然後按一下「自動完成」按鈕，最後取消「表單上的使用者名稱和密碼」功能。

如果使用Netscape Navigator，選擇「編輯」，「選項」，「進階」。從目錄中選擇「Cache」，然後按「Clear Memory Cache」及「清除自動儲存記憶」。

3. 發現可疑情況.....

● 留意是否如常收到銀行月結單或資訊，若有任何懷疑，應即時向銀行查詢

● 定期查閱銀行戶口結餘及交易紀錄。如發現任何錯漏或未經授權的交易，應立即通知銀行終止網上理財，與及其他可進入戶口的渠道如提款卡等

● 如收到異常的電郵並要求提供戶口資料或重要個人資料，切勿透露。如有疑問，即按銀行正式文件上列印的電話號碼，致電銀行查詢。不要使用電郵內提供的電話號碼

● 如對任何聲稱為銀行的網站產生懷疑，應聯絡金管局或警方

（hyper link）連接至其偽造網站。當客戶輸入用戶名稱和密碼，個人資料即時被盜取。騙徒利用有關資料進入真正的銀行網站，調動受害者的資產。

2. 偽造網站（fake websites）

設計與真銀行網站非常相似，市民若登上假冒網站，並輸入用戶名稱及密碼，騙徒即可讀取，利用這些資料在真正的銀行網站，進行投資交易及轉帳。

3. 其他手法

- 假冒銀行職員打電話要求客戶提供個人資料（pretext phone calls）
- 偷竊郵箱內銀行信件（post intercepting）
- 搜集被棄置在垃圾桶內的銀行月結單/信用卡收據（bin raiding）
- 偽造購物網站（bogus shopping websites）
- 以假讀卡機套取卡上資料（skimming）

二、消費者對損失的責任

發生假網上銀行騙案，令人擔心一旦個人資料外洩，戶口的存款會不翼而飛。

以銀行的網上個人理財服務為例，用戶一經登入，便可經網上買賣股票、外匯、基金及保險等，並可透過網上登記的個人帳戶支付款項，及申請信用卡。另外，亦可將戶口存款轉帳至他人戶口。現時銀行客戶一般可透過網上銀行轉帳至自己名下的其他戶口或已登記的他人戶口，不過，客戶事先要到銀行分行辦理指定轉帳戶口的手續，及只限轉帳至本港的銀行戶口。

本港兩間主要銀行設定已登記的他人戶口的最高每日轉帳限額為$100萬，客戶透過網上銀行轉帳至未經登記的他人戶口，每日最多$5萬。換言之，若騙徒透過假網站取得銀行客戶的登入用戶名稱與密碼，然後進入真正的網上銀行調走該客戶資金，每日最多可轉帳$5萬至在本港開立的銀行戶口。

若客戶存款只轉帳至在本港開立的銀行戶口，銀行方面理應可追查到有問題的轉帳。騙徒利用戶口轉帳盜款並不容易得手。當然，如果騙徒將存款電匯至外地，便有可能造成金錢損失。但為自保，**消費者宜考慮按實際需要調低網上轉帳限額，以減低可能的金錢損失。**

本會知道有銀行已着手加強戶口轉帳方面的保安措施——當客戶轉帳至未經登記的戶口時，銀行需要客戶輸入個人身份證明文件的其中幾個數字，以核對身份。本會歡迎銀行加強保障客戶的存款安全。

但如果騙徒在網上更改受害人的地址及電話，再申請信用卡寄到新地址，並用之購物，受害人便有可能損失金錢。**消費者要留意是否如常收到銀行月結單或資訊，若有任何懷疑，應即時向自己的往來銀行查詢及報告。**

在銀行與客戶之間會如何分擔因保安事故、系統故障或人為錯誤而引致的損失方面，**《銀行營運守則》列明，除非客戶作出欺詐或嚴重疏忽行為，否則客戶無須對其帳戶內任何未經授權交易引致的直接損失負責。**

三、網上銀行的監管

風險管理及資訊保安

金管局已實施了一套達國際水平的網上銀行監管制度，其中包括向認可機構發出網上銀行保安及風險管理指引。此外，本港的認可機構在推出電子銀行服務前，雖不用取得金管局正式批准，但要事先與金管局商討有關計劃及其風險管理措施，以確保認可機構作出足夠的資訊保安安排。認可機構並須外聘或委託內部獨立專家定期評估其電子銀行服務的資訊保安措施，當有關服務的風險評估出現重大改變或保安系統不能防禦入侵時，再作獨立評估。金管局並會在現場審查時，評估有關措施是否有效。在2003年金管局已進行了超過20次現場審查。金管局並於有關的認可機構推行了電子銀行及科技風險管理的自我評估機制。

金管局亦推行了一連串的工作，以協助防止及偵察虛假電郵與偽造網址騙案的發生。金管局在2003年5月發出「有關涉及虛假電郵或網站的海外騙案」通告（並於2003年8月再次發出該通告）提出了一些切實可行的方法。該通告建議**認可機構要確保其電子銀行客戶知道機構不會透過電郵要求客戶提供帳戶的敏感資料；認可機構亦要提醒電子銀行客戶如何確保他們是連接至機構的正式網站；認可機構亦可定期在互聯網上尋找，是否有任何第三方網站的域名可能會被誤會是該機構的域名，或是否有任何與該機構的網站建立了「超連結」的網站。**

此外，金管局、警方及香港銀行公會聯手推出一個多渠道消費者教育計劃，以提高公眾對電子銀行保安措施的認識。這個計劃包括印制教育小冊子，與及制作電視短片及電台廣播片段。**金管局內的「資訊中心」亦已裝置了互動電腦程式以教育公眾如何辨認虛假電郵及偽造網站。為方便消費者使用，本會建議金管局考慮在其網站內加入適用於網上瀏覽的辨認真假網站的資訊。**

在互聯網上的存款廣告

有關網上存款廣告的監管，金管局與其他主要金融中心的監管機構一樣，政策是只監管以香港市民為對象的網上存款廣告材料。

根據《銀行業條例》，境外註冊機構（包括虛擬銀行）若只邀請香港公眾人士在香港以外地區作出存款，則該機構毋須申請認可。但條例規定，任何邀請香港市民在香港境外作出存款的廣告材料，均須披露某些資料，當中包括有關的存款機構本身並未獲得認可，因此不受金管局監管。此舉確保有意在該機構存款的公眾人士，知悉有關事實，以便自行判斷是否將存款存入該機構。

《銀行營運守則》

對於在本港提供網上銀行服務的認可機構，金管局要求機構向個人客戶提供電子銀行服務時遵守《銀行營運守則》。《銀行營運守則》第六章內容包括：資料披露、保安問題、對損失的責任及匯報實際或懷疑保安事件。

認可機構提供的電子銀行服務應有足夠的透明度，讓客戶瞭解他們對有關服務可以有何合理期望，以及他們為保障有關服務的資訊保安而應採取的防範措施。除提供詳細的章則及條款外，認可機構應就電子銀行服務的使用備有一般說明資料（如費用及收費，及客戶就電子銀行服務的保安問題應負的責任等），供客戶查閱。

此外，認可機構應提醒客戶，他們有責任採取合理措施，確保接駁電子銀行服務所用的任何設備或密碼安全和保密。與此同時，認可機構應確保經其系統接收後，透過其電子銀行服務完成的交易是可追溯和查核的。

對損失的責任方面，認可機構應向客戶發出清晰明確的通告，提醒他們若損失是因他們的欺詐行為或嚴重疏忽（可能包括在知情情況下容許他人使用其設備或密碼）而引致，他們將要承擔所有損失。

認可機構應通知客戶向認可機構匯報或投訴保安事故的方法，以便能及早察覺、報告、回應及解決潛在保安事故或投訴。

四、本會建議

要推動香港發展電子銀行業務，先決條件是要建立安全穩健的環境，讓消費者放心使用網上理財服務。為此，**本會建議金管局考慮在認可機構名單內加入網址資料，方便消費者查證銀行網址的真確性。**而**銀行業方面，可考慮每當發現假網站等網上欺詐事件，盡快透過短訊或電子郵件發出e-Alert，通知網上銀行用戶，及定期提供最新的網上保安資訊。**