






You, your computer and the internet



Practical Tips

Millions of people are now taking advantage of internet banking and the convenience of being able to control their finances at any time, anywhere. Most banking and investment services are available online — all you need to do before you logon is take a few simple precautions.



1. You

-  Be alert — only open e-mails or attachments from known sources. Only download software from trusted sources.
-  Do not disclose your personal information online (e.g. HKID, address, bank account/credit card number) unless the site is both **secure** and reputable.
-  Check the website's privacy policy statement and statement on security safeguards before providing personal data to the website.
-  **SpooF websites** — always verify the domain name displayed on your browser's website address line, or access websites through your browser's bookmarks.
-  Change your online passwords regularly.




2. Your computer

-  Take personal responsibility for protecting your computer — limit the number of people who can use it and set your own password for your computer if it has this facility.
-  Install **personal firewall software** and **anti-virus software** and regularly download updates to **anti-virus software**.

3. The internet

-  Always disconnect from the internet when not using it.
-  Do not conduct transactions online unless the website is both **secure** and reputable.

4. Internet banking

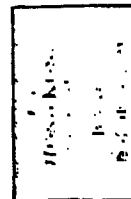
-  Select personal identifiers (e.g. user ID/ password) that are easy to remember but difficult to guess — do **not** use your birthday, telephone number or common names (such as girls' or boys' names and cartoon characters' names).
-  Do not disclose your password to anyone (**including bank staff and the Police**) and avoid recording it in your diary or computer.
-  Do not use your internet banking user ID or password for other online services (e.g. e-mail, internet access).

Internet Banking

Account


Number


OK




www.hkab.org.hk

 Review and follow the security tips published by your bank.

 Never access your internet banking website from a public computer (e.g. cybercafé) or through hyperlinks embedded in e-mails.

 Check your bank balance and transactions regularly – with internet banking you can do this any time 24 hours a day. You should notify your bank immediately if you discover any errors or unauthorised transactions.

 When a website claiming to be a bank looks suspicious to you, contact the Hong Kong Monetary Authority or the Police.

Banks and the Police will never ask you for your password. If you receive such a request, contact your bank immediately.

Personal firewall software and Anti-virus software – help block hackers and viruses from getting into your computer. Anti-virus software needs to be updated regularly to detect new viruses. Products available vary in features, support and price (certain products offer a free version for home use but with less features and support). More information can be obtained from vendors and the internet.

Secure websites – sometimes a tiny padlock or key icon will appear at the bottom of your browser. This indicates that the information you transmit to the website will be encrypted.

Spoof websites – a fake website which looks genuine by using similar graphics and domain name to those of the legitimate website. Double click the tiny padlock or key icon shown on your browser to check the digital certificate of the website. The certificate should be issued to the genuine domain name/organisation and have a valid date.

Enquiries

For any enquiries about internet banking, please contact your account-holding bank.

Useful links

- Information Technology Services Department:
www.infosec.gov.hk/english/general/protect/index.htm
- Hong Kong Police Force:
www.info.gov.hk/police/hkp-home/english/td/cd.htm
- Hong Kong Monetary Authority:
www.hkma.gov.hk
- Consumer Council:
www.consumer.org.hk

Issued by the Hong Kong Association of Banks and endorsed by the Consumer Council, the Hong Kong Monetary Authority and the Hong Kong Police Force.



消費者委員會
CONSUMER COUNCIL



HONG KONG MONETARY AUTHORITY
香港金融管理局



你、你的電腦及互聯網

實用貼士

數以百萬計的人士已採用網上銀行，享受隨時隨地理財的方便。大部份的銀行與投資服務都已在網上提供——你需要做的，只是在登入服務前，採取一些簡單的預防措施。

1. 你

- ☐ 提高警覺——只開啟從熟悉來源收到的電郵或附件，並且只從可靠的來源下載軟件。
- ☐ 切勿在網上隨便透露個人資料(如香港身份證號碼、地址、銀行戶口/信用咭號碼)，除非網站是安妥及信譽良好的。
- ☐ 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。
- ☐ 備置網站——時常核對瀏覽器顯示的網站地址，或使用瀏覽器上的書籤功能登入網站。
- ☐ 定時更改網上密碼。

2. 你的電腦

- ☐ 你有責任保護你的電腦——避免讓太多人使用你的個人電腦。可以的話，應設定使用電腦的個人密碼。
- ☐ 安裝個人防火牆軟件及防電腦病毒軟件，並定期下載防病毒軟件的更新檔案。

3. 互聯網

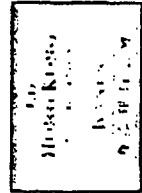
- ☐ 如已結束使用，應中斷與互聯網的連接。
- ☐ 只在安妥及信譽良好的網站進行網上交易。

4. 網上銀行

- ☐ 選用最易記但難被猜中的個人識別碼(如登入姓名及密碼)——切勿使用出生日期、電話號碼或常用的名字(例如小孩子的名字及卡通人物的名字)。
- ☐ 切勿向任何人(包括銀行職員及警方)透露密碼，並避免把密碼寫入記事簿或電腦。
- ☐ 不應使用進入網上銀行所用的登入姓名或密碼進行其他網上服務(如電郵及撥駁互聯網)。

網上銀行

安全理財



www.hkab.org.hk

☐ 遵照銀行提供的保安提示。

☐ 切勿使用公用電腦(如可供上網的咖啡室)或通過電郵的超連結登入網上銀行的網站。

☐ 定期查閱銀行戶口結餘及交易紀錄——使用網上銀行服務便可隨時查閱。如發現任何錯漏或未經授權的交易，你應立即通知你的銀行。

☐ 如你對任何聲稱為銀行的網站產生懷疑，應聯絡香港金融管理局或警方。

銀行及警方絕不會要求獲知你的密碼。假如你被要求透露你的密碼，應立即聯絡銀行。

個人防火牆軟件及防電腦病毒軟件——這些軟件有助阻止黑客及電腦病毒入侵。防毒軟件的病毒資料須定期更新，才能偵測新病毒。市面上產品的功能、支援水平和價錢都不盡相同(有些版本可供家用電腦免費下載及使用，但功能及支援會較少)。大家可從供應商及互聯網找到更多有關的資料。

安全網站——瀏覽器下方有時會顯示一個細小扣鎖或鑰匙的標誌，這表示你傳送到該網站的資料會受到加密技術的保護。

偽冒網站——偽冒的網站利用類似真實網站的圖像及網站地址，令人信以為真。你應在瀏覽器的細小扣鎖或鑰匙標誌上連按兩次滑鼠，以查閱網站的數碼證書。該證書應該是發給真正的網站地址/機構，日期亦應有效。

查詢

如有關於網上銀行的查詢，請聯絡你的往來銀行。

相關的網站

- 資訊科技署：
www.infosec.gov.hk/chinese/general/protect/index.htm
- 香港警務處：
www.info.gov.hk/police/hkp-home/chinese/tcd/tcd.htm
- 香港金融管理局：
www.hkma.gov.hk
- 消費者委員會：
www.consumer.org.hk

本單張由香港銀行公會發佈，並獲消費者委員會、香港金融管理局及香港警務處認可。



消費者委員會
CONSUMER COUNCIL



HONG KONG MONETARY AUTHORITY
香港金融管理局

