FOR MORE INFORMATION

LOG ON TO

www.bankinginfo.com.my

OR VISIT OUR KIOSK AT MOST BANKS

Second Edition

banking info
INFO PERBANKAN

E-TRANSACTIONS AND YOU

Internet Banking

A consumer education programme by:

BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

PERSATUAN BANK BANK DALAM MALAYSIA
THE ASSOCIATION OF BANKS IN MALAYSIA

contents

Date: 1 April 2007

Manage your finances

from just about anywhere in the world

Introduction

Internet banking allows you to manage your finances from home, work or from just about anywhere in the world. The purpose of this booklet is to provide information on Internet banking services offered by licensed banking institutions in Malaysia.

BANKING ON THE INTERNET

Currently, only banking institutions licensed under the Banking and Financial Institutions Act 1989 and the Islamic Banking Act 1983 are allowed to offer Internet banking services in Malaysia. A list of banking institutions that were granted approval by Bank Negara Malaysia to offer Internet banking services is available on Bank Negara Malaysia's home page www.bnm.gov.my.

FAST AND CONVENIENT

Internet banking provides you with a fast and convenient way to undertake various banking transactions during and after banking hours. Most banking institutions offer the service 24 hours a day, 7 days a week. You avoid travelling time and the need to wait in queues to access banking services or to pay bills.

WHAT IS NEEDED TO DO INTERNET BANKING?

Internet banking does not require special software or access to a private network, but is conducted through the Internet. If you have a computer with Internet access, a modem and telephone line, an Internet browser and have registered for Internet banking service with your banking institution, then you can conduct Internet banking from virtually anywhere in the world. It is recommended that you install a personal firewall and regularly update your virus protection software.

HOW TO APPLY TO BE AN INTERNET BANKING USER?

You can apply for Internet banking facilities if you have an account with a banking institution that offers Internet banking services. Details on the application procedures are available on the banking institutions' websites.

Fast and convenient
way to undertake various banking transactions

BANKING SERVICES AVAILABLE ONLINE

With Internet banking facilities, you will be able to perform a variety of banking transactions online. Depending on the banking institution, the main services offered through Internet banking allows you to:

- Check your balances and statements
- Submit applications for new accounts, credit cards or loans
- Place fixed deposits
- Transfer funds between accounts (own and third party)
- Pay bills, credit cards, loans and insurance premiums
- Create, change and cancel standing orders
- Request for cheque books and statements
- Check status or stop payment of your cheques
- Apply for bank drafts and telegraphic transfers

Some additional services offered include mobile airtime reload, interest rates calculator and foreign currency converters. Please check with your banking institution for the full list of services offered and the additional features and channels that are available.

BEFORE YOU SIGN UP

Prior to signing up for the service, you are advised to read and understand the terms and conditions of the service, which should provide:

- Information on duties of the banking institution and its customers
- Information on who will be liable for unauthorised or fraudulent transactions
- Mode by which you will be notified of changes in terms and conditions
- Information relating to how to lodge a complaint, and how a complaint is investigated and resolved

Measures are taken by banking institutions to ensure a **secure website**

You should also discuss with your banking institution the risks involved in using Internet banking services and to understand fully your rights and responsibilities.

IS INTERNET BANKING SAFE?

As in any other system, there are risks involved in Internet banking. However, potential risks are mitigated with banking institutions' continuous check on the security of the system and the care taken by you when using Internet banking services.

a. Actions taken by banking institutions to ensure security

In offering Internet banking services, banking institutions have invested considerable resources and efforts to ensure that their Internet banking set up is safe for consumers. In addition, banking institutions are also required to comply with the minimum guidelines issued by Bank Negara Malaysia. Amongst the safety measures taken by banking institutions are:

- Regular tests of the system to ensure its reliability
- Provision of security arrangements to ensure a secure infrastructure:
  - A number of security measures such as encryption, firewalls, automatic log-off and monitoring tools
  - A system to detect and disable attacks from hackers
- A two-factor authentication method that provides two levels of checking to validate the user
- Undertake a periodic review every 6 months to assess possible risks and detect possible weaknesses in the banking institution's risk management system

You can find information about the banking institution's security practices on its website.

b. Actions you should take to ensure security

You have an important role to play in ensuring the safety of Internet banking transactions. Some of the recommended actions that you, as a bank customer, should practise are:

- Do not reveal your login ID and password or PIN
  - Memorise it and do not write it down anywhere
  - Do not send any personal information particularly your password or PIN via ordinary e-mail
  - Do not store your login ID and password or PIN on the computer
  - Change your password or PIN regularly and avoid using easy-to-guess passwords such as names or birthdays. Ideally, your password should be a combination of characters (uppercase and lowercase) and numbers
  - Do not respond to any request for your login ID and password or PIN over the phone, through fax, e-mail or pop-up message, no matter how official or important it may seem
  - Change your password or PIN immediately and notify your banking institution if you suspect any unauthorised use of your accounts or that someone else may know your password or PIN
  - Check your transaction history details and statements regularly to make sure that there are no unauthorised transactions on your accounts or additions to the list of registered payees
- Check for the right and secure website
  - Always enter the URL of the website directly into the web browser. You should avoid being re-directed to the website, or hyperlink to it from an e-mail or another website

- Make sure that you are in the correct website before doing any online transactions or providing personal information
- Ensure that you are in a "secure" website by checking the Universal Resource Locators (URLs) to ensure that it begins with "**https://**" instead of "http://" and look for a display of a closed padlock symbol on the status bar of your browser. However, you are cautioned that the URL and the closed padlock symbol, which represents the Secure Sockets Layer (SSL) certificate, could also be forged. Therefore, you should exercise greater vigilance by checking the URL and the SSL certificate from the 'Page Properties' tab to confirm the authenticity of the website
- Install a web browser toolbar that alerts you of any known phishing fraud website to minimise the risk of falling into phishing scams

- Subscribe to a better user authentication methodology
  - Sign up for two-factor authentication method with your banking institution to add a second level of authentication and secure your transaction
- Protect your personal computer from hackers, viruses and malicious programmes
  - Install a personal firewall and a reputable anti-virus programme to protect your personal computer from virus attacks, spyware or malicious programmes such as "Trojan Horse"
  - Ensure that the anti-virus and anti-spyware programmes are up-to-date and are running at all times
  - Keep your operating system and web browser up-to-date with the latest security patches in order to protect against weaknesses or vulnerabilities
  - Configure your browser to reject ActiveX controls to reduce the likelihood that spyware could be installed on your computer

- Be careful when downloading software
  - Always check the programme or attachment received with an updated anti-virus programme to ensure that it does not contain any virus that could attack your computer
  - Never download any file or software from sites or sources, which you are not familiar with or click on hyperlinks sent to you by strangers. Opening such a file, software or hyperlink could expose your system to a computer virus that could hijack your personal information, including your password or PIN
- Do not leave your computer unattended when logged in
  - Log-off from the Internet banking site when you leave your computer unattended, even if it is for a short while
- Always remember to log-off
  - Always log-off when you have completed your banking transactions

- Clear the **memory cache** and **transaction history** after logging out from the website to remove your account information. This would avoid stored information from being retrieved by unwanted parties

- Other measures
  - Do not have other browser windows open while you are banking online
  - Avoid using shared or 'planted' or public personal computers, e.g at Internet cafes, to conduct your Internet banking transactions
  - Disable the "file and printer sharing" feature on your operating system
  - Contact your banking institution to discuss any security concern you may have on your online accounts, including remedies required

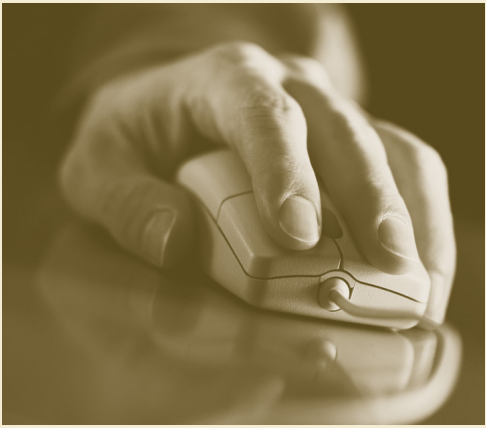
INTERNET SECURITY THREATS

You are encouraged to continue educating yourself on emerging Internet frauds from sources such as the online advisories of your banking institution's website and from industry groups' websites dedicated to eliminate online frauds.

Be careful
when downloading software or receiving a programme or an attachment

You should stay vigilant for new threats, including phishing, pharming and man-in-the middle attack.

Phishing is the act of sending spoofed e-mail messages falsely claiming to be from your banking institution to lure you into divulging personal information such as PIN or password for the purpose of identity theft. It often contains a link to a website that contains logos, formatting, graphics and wordings that are convincing replicas of the banking institution's original site.



Read the
privacy policy
statement posted on your banking institution website

Pharming is the act of exploiting the vulnerability of the Domain Name System (DNS) server software that allows a hacker to acquire the domain name of banking institution's original site and redirect traffic from the banking institution's site to a fraudulent site.

Man-in-the-middle attack is an attack in which fraudsters are able to read, insert and modify messages between you and your banking institution without either party knowing that the link has been compromised.

You may minimise the risk of being a victim of these Internet frauds if you undertake the measures listed in "Actions You Should Take to Ensure Security". You should also be suspicious of any e-mail with contents or urgent request for your financial information as phishers typically include upsetting or exciting (but false) statements in their e-mails to get you to react immediately.

PRIVACY OF YOUR PERSONAL INFORMATION

Both banking institutions and you have a role in ensuring privacy. Protection of your personal and financial information is an extremely important matter when banking via the Internet. The privacy of aconsumer's personal information to be an important element of public trust and confidence in the banking system.

a. Responsibilities of banking institutions in ensuring privacy

All banking institutions offering Internet banking services have to adopt responsible privacy policies and information practices. For example, banking institutions should prompt you with a message to inform you that you will be leaving the banking institutions' websites and hence you will not be protected by the privacy policies and security measures of the banking institutions when you hyperlink to third parties from their websites.

b. Your responsibilities in ensuring privacy

You are advised to read the privacy policy statement of banking institutions, which are posted at their websites prior to providing your personal information. By reviewing this policy, you will know the type of information banking institutions collect and maintain about you. Banking institutions may want to share information about you with a related entity to market specific products that may meet your needs and interests. If you do not want your banking institution to share your personal information with others without your permission, you should request your banking institution for the "opt out" option.

Which banking institution offers Internet banking services?

Generally, banking institutions offer the service to bank customers with existing bank accounts, credit cards or loans. There are also banking institutions that offer special accounts designed for Internet banking for existing as well as new customers. A list of approved banking institutions offering Internet banking facilities is available in Bank Negara Malaysia's website **www.bnm.gov.my**. You are advised to sign up only with licensed banking institutions approved by Bank Negara Malaysia to offer Internet banking services.

What are the accounts that I can access through Internet banking?

You would be able to have access to the accounts that have been linked to the service. This could be your savings, current, fixed deposit, loan and credit card accounts.

What do I need to access Internet banking?

You will need an Internet-enabled device such as a personal computer with a suitable operating system, Internet access via a modem and a suitable web browser. More details on these may be found on the banking institutions' Internet banking web pages or by contacting the banking institutions.

What does it cost to use Internet banking services?

Subscription to the Internet banking services is currently free, although this may change depending on the banking institutions. Fees may also be charged for some services such as interbank fund transfers, telegraphic transfers and requisition for new cheque books. Do check with your banking institution to find out more about the fees imposed. Competitive fee structure may apply for using the Internet to conduct your banking activities as compared to using other channels such as branch counter service. Some banking institutions also offer Internet banking services to their corporate customers and subscriptions to such services may be charged.

What are the steps that I, as a consumer, can take to make Internet banking more secure?

Internet banking offers a safe way to conduct your banking transactions when adequate security precautions are taken. You are advised to:

- Keep your login ID and password or PIN confidential
- Change your password or PIN regularly
- Refrain from storing your login ID and password or PIN on the computer
- Check that you have logged into the right website
- Check your transaction history details and statements regularly
- Refrain from leaving your computer unattended, while connected to the Internet banking service
- Sign-off at the end of each session and clear the memory cache and transaction history after logging out from the website

- Protect your personal computer from viruses and malicious programmes by installing an up-to-date hackers firewall and a reputable anti-virus and anti-spyware programme. These programmes must be updated regularly to be effective. Although some anti-virus programmes may have anti-Trojan Horse features, it may remove only the more popular Trojan Horse programmes. You may want to consider installing an anti-Trojan Horse programme which is specifically designed to scan and remove any Trojans from your computer
- Avoid downloading files or software from sites, which you are unfamiliar with or click on hyperlinks sent to you by strangers
- Avoid sending any personal information particularly your password or PIN via ordinary e-mail
- Avoid using shared or 'planted' or public personal computers, e.g at Internet cafes, to conduct your Internet banking transactions

What if something goes wrong or I made a mistake?

If you encounter any problem, contact the customer service department of your banking institution immediately with details of the transactions and problems encountered. Your banking institution will have records of all your transactions and they will be able to assist you on this matter.

Who bears the loss when things go wrong?

The contractual arrangements for liability should provide for sharing of risks between the banking institutions and their customers. Customers should not be liable for losses that were not caused by them provided they have not acted negligently. However, you are responsible to keep your login ID and password or PIN confidential and undertake the necessary security measures as advised in "Actions You Should Take to Ensure Security" above.

Where do I turn to if I have a complaint or would like a dispute resolved?

You should contact your banking institution if you have any complaint. All banking institutions have set up a dedicated Complaint Unit to deal with customers' complaints. Information on the contact person, telephone number and e-mail address is available on Bank Negara Malaysia's website at **www.bnm.gov.my**.

For more information on how to make a complaint against a bank, please read the BankingInfo booklet on "Making a Banking Complaint."

GLOSSARY

ActiveX
A software technology that has a set of rules on how applications should share information which allow programmed capabilities or content to be delivered to Windows-based personal computers via the Internet.

Web Browser
A web browser is a software programme used to surf the web. It enables users to visit websites and view web pages on their personal computer screen. The browser handles all the work that goes into viewing web pages.

Cache
A cache is the memory a browser uses to store content of web pages that has been visited. Storing that content allows the browser to load those same pages more quickly the next time the same user visits them.

Encryption
Encryption is the process of scrambling data into an unreadable format that is more secure for transmission over the Internet. Encryption is used to prevent the risk of the information being intercepted and read by a third party. The most common encryption technology is Secure Sockets Layer (SSL) which automatically encrypts all traffic between your website browser and the servers. You can tell you are in SSL encrypted website by looking at the URL which will begin with https://. There are two levels of SSL encryption which are 40-bit and 128-bit. The 128-bit browsers provide the highest level of security available today.

Firewall
A firewall acts as a filter that prevents information from getting in or out of a protected network.

Trojan Horse
A programme that appears to be useful or harmless but actually hides malicious or harmful code designed to exploit or damage the system on which it is run.

Two-Factor Authentication
A process to verify the identity of a person through validating two credentials provided. The two credentials are typically something a customer knows, i.e. login ID and password, and either something a customer has, e.g. digital certificate and one-time password generated by tokens or provided via short message services or something a customer is, e.g. biometric features such as fingerprint or retinal pattern.