

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.

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.

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.

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



Internet banking

on the security of the system and the care taken by you when using Internet banking services.

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.

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.
- 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 antispyware 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.