Security Statement

Security standards employed by us—and what you can do to stay safe online

The WPN (mywpn.com) is highly committed to ensuring that all transactions performed through our online financial service are secure, safe and confidential. For this purpose, we enforce privacy protection control systems designed to ensure the highest security standards and confidentiality.

- Username and password>
- Information protection>
- Data confidentiality and data integrity>
- Systems security and monitoring>
- Computer virus protection>
- Updating your browser>
- Security tips>

Username and Password

To prevent unauthorized access to our online financial services, every customer is required to select a username and an alphanumeric password, which provides access to their financial information. The username must be between 6 to 16 characters and the alphanumeric password between 8 to 12 characters. The password must include both alphabets and numbers but you may also use special characters (e.g. & * $) except spaces.

The username and alphanumeric password are case sensitive. For example, if your password is "fuNNySAD2B" and you key in "fuNNySAD2b", you will not be able to login (the "b" must be uppercase).

Here are some tips to ensure the integrity of your username and password:

- Do not choose a password that others can easily guess.
- Do not use simple words, your name, birth date, telephone number or names listed in a standard dictionary.
- Memorize your password and do not write it down.
- Passwords or PINs should be used when accessing an online account to protect your personal information.
- Sharing your password or PIN with another person is the same as giving that individual authority to use your name in a transaction. **It should not be disclosed even if requested by an authorized Mywpn Officer**.
- Change your password frequently.

To create a unique password, try the following methods (but don't copy the examples):

- Use a combination of unrelated words and numbers
- E.g. tiger63rain
- Use grossly misspelt or mistyped words
- E.g. sinaran_07 —: slnalam_07
- Use both upper and lower case characters
- E.g. funnysad2b —: fuNNySAD2B
- Use a line of lyrics or poem
- E.g. "A thousand sad reasons for a broken heart" —: 1Ksrfabh

Information Protection

While we take considerable effort to ensure a safe and secure online experience, we have no control over the computer you use to access Mywpn.com. As an added security feature, we have incorporated an automatic log out function if no activity is detected after a preset time limit.

However, you must ensure you do not provide anyone the opportunity to gain access to your account information:

- Ensure no one has access to your computer or records your online activities.
- Always log out of Maybank2u.com immediately after completing transactions and before visiting other websites.
- Do not send any information about your account via e-mail.
- Disable the AutoComplete function on your browser to avoid automatic completion of your ID when you type in User ID.

To turn AutoComplete "**On**" or "**Off**" in MS Internet Explorer browser:

1 Click the "Tools" menu and select "Internet Options.
2 Click "Internet Options" to get the "Content" tab.
3 From this tab, click the "AutoComplete" button.
4 Uncheck "User names and passwords on forms".

Mywpn.com collects personal information that you voluntarily provide on this Web site, which may include your name, address, e-mail address, marital status, salary range, number(s) of children, etc. We use this information to communicate with you and to provide you with your requested service or product. If you provide your consent at the time your personal information is collected via this Web site, we may also provide you with information, special offers, and promotions. Furthermore, we may store some or all of that personal information and use it for marketing research and marketing purposes. We maintain your data for as long as you are a customer of the Mywpn. Personal information shall be retained by the Bank in accordance with the current law and regulatory requirements.

Data Confidentiality and Data Integrity

An EV SSL certificate offers the highest available levels of trust and authentication to your website, designed to strengthen e-commerce security and combat phishing attacks to make EV SSL the most complete SSL certificate available. The green address bar prominent displays the Bank’s name and provides highly visual assurance to customers ensuring that the site is secure. It also provides immediate trust and helps customer conversion with 2048 – bit and highest assurance SSL Certificate.

Systems security and monitoring Systems security and monitoring

The Mywpn has adopted a combination of the following systems security and monitoring measures for online transactions:

- Firewall systems, strong data encryption, anti-virus protection and round-the-clock security surveillance systems to detect and prevent any form of illegitimate activities on our network systems.
- Regular security reviews of our systems by our internal System Auditor as well as external security experts.

- When you have a broadband connected to the Internet (always-on connection), consider installing a personal firewall. At a minimum, power-off your PC when not in use.

We also take every effort in ensuring collaboration with major vendors/manufacturers to keep abreast of information security technology developments, for possible and future implementation.

Computer virus protection

Computer viruses are real and once your computer is infected it can cost you time, loss of information, repair expense, and aggravation. Make sure your computer has an anti-virus protection program installed to reduce the risk.

We recommend that you purchase a program that automatically upgrades your virus protection on a recurring basis. If you currently have a virus protection program on your computer without the automatic upgrade feature, make sure you update your virus detection program at least monthly and/or when you hear of a new virus to minimize your risk. You can do this by visiting the Internet site of the company that provides your software.

In addition, we advise you not to open attachments from others unless you are absolutely certain you can trust the source. However, it's best to be cautious. Whoever sent you that attachment may not know that they have carried the virus to you.

Updating your browser

An Internet browser allows access and the ability to navigate a myriad of information and service resources on the Internet. Most computers come with a browser already installed.

- Always update your browser when new versions are released because they often include new security features.
- Check your browser for built-in safety features that you may or may not elect to use.
- If you use Internet Explorer, update it to IE version 8.0 and above.
- It is a good practice to always check the site certificate before login

Security Tips
Protect Yourself and Your Information Online

Be careful when you do your banking online. There have been cases of copycat web sites created by unauthorized persons posing as authentic web sites, or e-mail/phone calls asking you to provide personal or account-related information with the intention of carrying out Internet theft and fraud.

Please take necessary precautions and be on the alert for suspicious e-mail or phone calls asking for your personal account information. **Never reveal your Internet Banking or ATM PIN or account information to anyone.**

10 easy ways to protect yourself

1 Do not share your password with friends, relatives or **anyone**. Your

password and PIN are designed to protect the privacy of your banking information. They will only work if you keep them private.

2 Change your password frequently. If you think your password has been compromised, contact us to reset your password.

3 Don't use the "remember password" function because this information can be easily accessed by hackers.

4 Do not send any information about your account via e-mail.

5 Do not provide your account details or passwords in response to an e-mail or by phone. A bank officer will never ask for this information.

6 Don't open suspicious e-mail attachments.

7 Avoid downloading free programs. These may incorporate hacker-friendly software.

8 Always log out of Mywpn.com immediately after completing transactions and before visiting other web sites.

9 Clear your cache (information stored in your computer memory) each time you log out.

10 When using the Internet Banking Kiosk, **logout and return to the Home Page** before leaving the kiosk.

If you have queries about any e-mail from Mywpn or are suspicious that someone may be trying to get your PIN or account information under false pretenses, contact **our Customer Care hotline at** +371 22033273 immediately.

Last Update: 1 April 2018