Tips on How to Protect Yourself Online

1. **Create a robust user password**

   It is important for the user to create a robust password. For greater security, the password should be in line with our stricter password rules, that is,

   - It must be a combination of both letters and numbers
   - It can have a length of 8 to 12 characters
   - It is case-sensitive
   - No special characters (e.g. #!$%^) and spaces are allowed, except underscore

2. ***Do not disclose the password to anyone***

3. ***Do not use easy-to-remember dates or numbers to create the password***

4. ***Do not use the same Internet Banking password for other online accounts***

   It is dangerous to share the same password for other online accounts as most non- banking systems provide easy access for password recovery.

5. ***Do not write down or store the password***

   - Avoid writing or storing the password in easily accessible items like a notepad or the PC
   - Do not select the option on browsers for storing or retaining username and password

6. ***Do not access Online Banking from computers or devices which cannot be trusted***

7. ***Do not access Online Banking for Company Account from public areas***

   Do not access Online Banking for Company Account at cyber cafes, which are prone to attacks from "Trojan Horse" or other malicious programmes.

8. ***Log off your online session when not in use***

9. ***Always clear the browser's cache memory (delete browser history) after each online session***

10. ***Take note of the last login time every time login***

    Do make it a habit to check the last login message whenever you login, as it tells you when the last login was performed.

11. ***Check your transaction history details regularly***

    This will help you keep track of your account activities. If you notice any discrepancy, contact Maybank immediately.

12. ***Do not save the Bank's URL on the browser's Bookmark or Favourites***

    Access the Bank's web site directly by entering the URL in the browser's address field.

13. ***Protect yourself from fraudulent/phishing emails and web sites***