STATE BANK OF INDIA

Password creation and maintenance

The following rules regarding passwords have been built in the Internet Banking application

- Password to contain a minimum of 8 and a maximum of 28 characters, with no spaces in-between.
- Password to contain one alphabet, one numeral and one special character
- Password can not consist of all characters of user-id.
- Changed password can not be same as any of previous 3 passwords.
- If the customer does not log into Internet Banking for more than 180 days, he will not be able to log-in. He has to request the branch to reset his password.

Customers are also advised to take note of the following ;

 Ensure that no other person gains knowledge of your User-Id, Password or the digits on your scratch card.

 Enter your user-id password only in the space provided for that, which you are normally used to.

 The user shall avoid storage in storage media of the data terminal used by the User (e.g., personal computer). The user ID communicated to the User in writing and the scratch card shall be imperatively stored in a safe place which cannot be accessed by third parties. The user ID and the password must not be stored together with the scratch card.

 Do not provide user id passwords on any page popping up by clicking on a hyperlink received through email. Better practice would be to log into the service by typing in the URL in the address bar after making sure the page opening up is from the genuine service provider.

 When entering his/her user ID, password and the digits from the scratch card the User shall ensure that these cannot be seen by other persons. The user ID, the password and the digits from the scratch card may be transmitted to the Bank only by means of the online banking access channels notified by the Bank.

 Change password **at least** once in 6 months.

 Unique Characters: A strong password should have at least five (5) different characters. Repeated characters can make for palindromes and make it easier to crack.

- Character Types: A strong password should have characters from at least three (3) different character types -- upper case, lower case, digits, punctuation, etc. A password that includes a sample from a rich character set is difficult to crack.

- Long Alpha Sequences: A good password must not have an alphabetic sequence any longer than three (3) characters.

- Long Digit Sequences: A strong password must not have a digit sequence any longer than two (2) characters.

- Forbidden Characters: There are a few characters that will cause problems if used in a password - the "delete" character is one of the obvious ones.

- Writing down your password: One should never write down a password. Someone may discover the password. Make the password difficult for others to guess or crack but easy for you to memorise and remember.

- Passwords should not be any of the following:

    - Dictionary words (including foreign and technical dictionaries)

    - Name of a person or a thing, a place, a proper noun, a phone number or a vehicle number

    - Simple pattern of letters on keyboards

    - Any of the above reversed or concatenated

- One possible method for picking a good password is to make up your own acronym.

- Do not let your computer remember your password . Do not accept auto complete option provided by your computer/ browser.

- As far as possible do not use un-trusted system to access sensitive service. If you must, change the password on the first occasion immediately thereafter from a trusted system