



Your Money is safe with Bank,  
Yet.....A little extra care makes your  
online transaction more secure

The convenience of online banking which has to be used with care to prevent rude shocks by way of any frauds. Need of the hour is that one has to be aware of “Phishing”.

An online method used by fraudsters to steal customer’s personal details like User IDs, Passwords, Date of Birth, CVV, IPIN, Credit/Debit Card No., Card Expiry Date and so on.

#### What is “Phishing” .....How to prevent it.

- Fraudsters can get personal information from Bank’s customer through emails or phones. These are very cleverly camouflaged and appear to be originating from the bank self.
- Information could also get siphoned off while you are logged on to your bank’s website. This happens through pop-ups, which appear alongside your bank’s webpage asking unsuspecting users to disclose confidential information.
- Other requests might draw you to be part of survey or inform you that your online session has expired and that you need to validate/update/reveal your account to revive it.
- This could also happen when you download software or files from an unknown source or through threats that your online session will be shut down if reconfirmation of account details is not carried out.

#### Care to be taken to remain out of phishing trap

- Always type the address of your bank URL in the browser bar only.
- Avoid opening of multiple windows during a session.
- Remember Bank’s never ask Personal information over phone/email. Please don’t entertain such mails/calls.
- Always log off systematically and reconfirm your status.
- Use proper updated anti-virus and anti – spyware tools to keep your computer healthy.
- Employ dual security passwords for added protection.