बैंक ऑफ महाराष्ट्र Bank of Maharashtra भारत सरकार का उद्यम एक परिवार एक बैंक	**Integrated Risk Management Department** **Head Office, Pune - 411005**

Dear Valued Customer, 12.12.2019

Thank you for banking with Bank of Maharashtra!

Security of your account is of utmost importance to us. In our endeavour to continue educating our customers on security, we are hereby publishing the Customer Awareness - 9. Please find the same below. Hope you will find it useful and informative.

Customer Awareness – 9

PROTECT YOURSELF FROM SOCIAL ENGINEERING FRAUDS

Fraudulent phone calls and SMSs containing fraudulent URLs on the subject of KYC updation, linking of bank accounts, seeking confidential information of customers, are currently in circulation.

These are the attempts made by the fraudsters to siphon the money from the bank accounts of innocent people. Therefore, keep yourself safe from banking frauds and learn the tricks to avoid Social Engineering frauds.

PHISHING:

- Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers.

VISHING:

- Vishing is also a type of social engineering attack in which a cybercriminal contacts the customer by phone, impersonating someone in a position of authority. Vishing is similar to phishing, but the attack is delivered by phone instead of via email.

SAFETY TIPS:

1. Be very cautious of any caller who asks to share login information over the phone/email.
2. If a caller asks to provide account data or personally identifiable information, refuse to do so.
3. Do not download and execute any mail attachment received from unknown source.
4. Do not transfer funds to or share account details with unknown / non-validated source.
5. Do not respond to E-mails/SMS claiming to be from Bank and seeking any confidential personal information.
6. Report impersonated or suspect email or any suspicious call received.
7. Use updated and licensed Anti-Virus software.
8. Be aware of fraudulent activities on Internet.

In case you receive SMS related to KYC updation, please do not respond to it. It can be fraudulent. Fraudster generally ask for DoB, Mobile no, e-mail id through SMS link. We request you not to give any such information. Bank never ask for such information.

By Chief Information Security Officer
Bank of Maharashtra