Cyber Security TIPS
for protecting yourself online

1. KEEP YOUR COMPUTERS & MOBILE DEVICES UPDATED
Always keep updated operating system, browsers, anti-virus software of computer / laptops / palmtops / tablet / smart phone and other devices used by you. Turn on automatic updates so you receive the newest fixes as they became available. It gives very strong protection against viruses, malware, and other threats.

2. USE OF ANTI VIRUS SOFTWARE
Always install a good quality paid Anti-Virus / malware software in your device.

3. SET STRONG PASSWORDS
Always set strong passwords. A strong password is at least 8 characters in length and incudes a mix of capital(A-Z) & lower case (a-z) letters, minimum one number (0,1....9) & minimum one special character (@, #, $, %, etc).

4. DO NOT SHARE YOUR SENSITIVE FINANCIAL DETAILS
Bank does not ask accounts number, debit, or credit card number, CVV number, Expiry date, PIN, OTP, mobile or internet banking login, password, MPIN or TPIN personally or On call or through email. Never share this information to anybody on phone / SMS / email.

5. KEEP PERSONAL INFORMATION PERSONAL
Hackers can use social media profiles to figure out your passwords and answer security questions to reset your password. Lock your privacy settings on social media profile and avoid posting things like birthdays, address, mother name, etc. Do not answer to request from unknown person.

6. SECURE YOUR INTERNET CONNECTION
Always protect your home & office wireless network with a strong password. Be cautious while using public Wi-Fi networks.

7. SHOP SAFELY
Always make sure that online shopping site you are using is official & secured. In checkout screen verify that the web address begins with **https://** and check to see padlock symbol appears on the page.

8. WATCH OUT FOR PHISHING SCAM
Phishing scams use fraudulent emails and websites to trick users into disclosing account, login, personal & KYC information. Do not click on links or open any attachments or popup screens from unknown / unrecognized source.

Customer Alert !!! [Beware of phishing]

[DO'S AND DONT'S]

Phishing is a fraudulent attempt, usually made through emails/calls/SMS to capture your confidential data like NetBanking Id / Password, mobile no, email Id/Password, Card no/PIN/CVV no, Mpin / Tpin etc.

Do not respond to fraudulent communications asking your confidential like A/c No, User Id, Password, Card No, etc

Fraudulent e-mails contain links of look-alike websites to mislead into entering sensitive financial data

Bank will never send such communications to customers asking for their personal or confidential information

Always visit Bank's site instead of clicking on the links provided in emails or third party websites

Do not respond to pop-up windows asking for your confidential information

X	**Bank will never send you e-mails asking for confidential details of your account/ PIN/ Password or personal details.**
X	**Never respond to e-mails/embedded links/calls asking you to update or verify UserIDs/Passwords/Card Number/CVV etc**
X	**Never click on any links in any e-mail to access the bank's site.**
X	**Never enter login or other sensitive information in any pop up window.**
X	**Do not be victim of SIM SWAPS, immediately investigate when you notice that you are not receiving call and message or getting SIM Registration fail. Keep your phone switched on and check alerts from Bank.**
X	**Never respond to any SIM Swap Request even from mobile operators.**
√	**Access your bank website only by typing the URL in address bar of browser.**
√	**Always check the last log-in date and time in the post login page.**
√	**Immediately change your passwords if you have accidentally revealed your credentials.**
√	**Please report immediately on phishing @ www.dharatibank.com if you receive any such Phishing email / SMS or Phone call.**