ONLINE SECURITY TIPS

PHISHING & PASSWORD PROTECTION

Phishing, also called spoofing, is the act of attempting to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business with a real need for such information in a seemingly official electronic notification or message. The e-mail directs the user to visit a web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers that the legitimate organization already has.

Bank of Baroda sincerely requests you to read and implement following Instructions to protect yourself from Phishing :

1. Never respond to emails that request personal information
At Bank of Baroda, we would never ask for your personal details through an email/ phone. Nor would we ask for your password through any means, online or offline.

2. Always check the URL and the Security Certificate.
Baroda DigiNext is hosted on secured site: https://barodadiginext.com/iportalweb only. While clicking on Login button, do not forget to check the URL on the Address Bar. Also, at any point, you can reassure yourself by cross checking the security certificate. This can be viewed by clicking on lock icon on status bar at the bottom.

3. Avoid using cyber cafes to access your online accounts as they may be infected with Virus, Trojans or Spywares which might track your activity or worse, compromise your security.

4. Keep your computer secure by installing and continuously updating Anti-Virus software(s).

5. Keep your password top secret and change it often.
Please do NOT disclose your User ID and/ or Passwords to any person – not even Bank staff – either intentionally or otherwise. Periodically change your Passwords.

How does Baroda DigiNext protect you from Phishing

Bank, on their part, use 256-bit Secure Sockets Layer (SSL) encryption technology certified by Verisign to https://barodadiginext.com/iportalweb to encrypt the information you send online. This ensures that the information exchanged between your computer and the Bank's web site is completely protected and all details such as login and password remain secret. Another safety feature is the timed logout, which means the session is automatically terminated if it is not active for a certain period.

BRIEF ABOUT YOUR PASSWORD:

As per existing arrangement, you will receive user id on your registered mail and your registered mobile number. First part of the login password will be sent on your registered e-mail id and second part on your registered mobile number (Mode of delivery of User ID and Password is subject to review from time to time, at the discretion of the Bank). You will have to compulsorily change the password, when you log in for the first time. While changing the password and while subsequently using it, please note that :

- It must contain **minimum** 8 digits and **maximum** 16 digits.
- It should not contain all the letters used in your User ID.

- To make the password complex and difficult for others to guess, the customers should use a combination of any three : Upper case character / Lower case character / Numeric character / Special character
- It is case sensitive i.e. if password is in small letters use the same. If you use capital letters, it will not work & vice-versa.
- For your safety, your user id will be blocked, in case of 5 failed attempts to log in. To enable the user id and regenerate the password, please contact your base branch/ DigiNext Operations team.
- While changing the password subsequently, you can’t use any of your last 5 passwords.
- If not changed in 90 days, system will force you to change the password. However, we advise you to keep changing the passwords, at regular intervals.
- If you have forgotten your user ID then please contact your base branch/ DigiNext Operations team.
- If you have forgotten your password, the same can be reset using Forgot Password option available on the login page. An OTP will be sent on your registered mobile for this purpose.

For each and every transaction, you will receive an OTP on your registered mobile number.

SECURITY OF YOUR PASSWORD:

Please note that your password(s) are of utmost importance in Baroda DigiNext. It is the only way that the system can identify you. Therefore, its security is very crucial and we advise you as under:

- Please do not write down these passwords anywhere.
- If you feel someone has obtained any of your passwords (i.e. it is compromised), please change the password immediately.
- Change the passwords at regular intervals (you will be forced to change the password by the system after 90 days).
- Do not share your username and password(s) with anybody, including Bank staff. (Bank does not require your user id or password at any point of time. So if you receive any communication asking for this information, please do not send your user id or password(s)).
- Do not use name of your spouse, children etc. as passwords, since they are very easy to crack. Further, avoid using important dates (wedding anniversary, birthdays of yourself/ spouse/ children etc.) as your password. Also, avoid relative’s name or date of birth or address in your password.

OTHER IMPORTANT SECURITY TIPS:

- Do not leave your computer unattended while accessing Baroda DigiNext.
- Always type full URL https://barodadiginext.com/iportalweb or add this website in your favourites which will eliminate the need for typing the URL every time you log in and subsequent risk of scouting.
- Every time you log in, your last login time is displayed. If you feel that you did not log in at the time shown, become alert immediately. Change your passwords, check all transactions and ensure that nothing untoward has taken place.
- Please ensure that antivirus on your PC is updated; thereby risk of virus attacks can be reduced. However, anti-virus cannot check for spywares. So avoid downloading unwanted software from unreliable websites.
- The recommended browser is Internet Explorer Version 11 and above
- As and when you have finished using Baroda DigiNext, do not forget to log out completely. Further, close the window completely after you log out. Avoid closing the window abruptly after usage.

- Know your software. Malicious software (e.g. viruses, worms, Trojan horses, and spyware) often masquerade as legitimate and even useful software. Think carefully before installing or running new software, especially anything unsolicited.
- Clear the browser cache regularly. To clear your browser cache in Internet Explorer:
    - Go to "Tools"
    - Go to "Internet Options"
    - Select "General"
    - Click on "Delete Files" in "Temporary Internet files" tab.