



BGGB: HO: IT-SEC: 02/144

Date: 25.06.2020

**CIRCULAR TO ALL BRANCHES / OFFICES**

Madam/Sir,

Increased digitization is exposing banks to more and more new and emerging threats. Hence banks need to deploy robust security controls without compromising customer experience. IT Department of our bank has time to time issued various circulars governing information security best practices to be followed by employees and customers.

We refer RBI circular RBI/2019-20/256 DPS.CO.OD.NO.1934/06.08.005/2019-20 dated 22-06-2020 regarding Increasing instances of Payment Frauds – “Enhancing Public Awareness Campaigns through Multiple Channels”. Fraudulent attempts are increasing day by day through Phishing & Vishing and other techniques to acquire sensitive personal and financial information such as user name, passwords, OTP, PIN, card details, etc by masquerading as a trustworthy entity in an electronic communication. Communication purporting to be from trustworthy organizations like banks, credit card companies are commonly used to lure the unsuspecting customers. These activities typically carried out by e-mail or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate site.

**What to Do:-**

1. Check the source of information from all incoming mail.
2. Enter sensitive data in secure websites i.e. the website must begin with `https://` and your browser should have an icon of a closed lock.
3. Check the language and spelling of the text contained in the e-mail.
4. Always type the website address in your web browser address bar without clicking on the link directly.
5. Use a caller ID option in the telephone, if available.
6. Ask questions, If someone is trying to sell you something or asking for your personal or financial information, ask them to identify who they work for and then check them out to see if they are legitimate.
7. The longer the password, the tougher it is to crack. Use at least 8 characters (combination of letters, numbers and special characters).
8. Be careful about shoulder surfing while entering your password

---

**HEAD OFFICE**

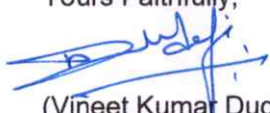

3<sup>rd</sup> & 4<sup>th</sup> Floor, Suraj Plaza- I, Syajiganj, Vadodara-390005 (Gujarat), INDIA  
Email – [ho@barodaqujaratrb.co.in](mailto:ho@barodaqujaratrb.co.in), website – [www.bgggb.in](http://www.bgggb.in)

**What to Avoid:-**

1. Never click on a link given in an unsolicited e-mail from unknown and suspicious sender.
2. Do not open unexpected email attachments or instant message download links
3. Do not use your official email address for social media sites.
4. Do not forward or reply to chain or spam mails.
5. Never answer a call from an unknown suspicious number.
6. Even if you answer, do not share sensitive information over a phone call with anybody, even if he/she claims to be from the bank. Bank never asks for personal information over the call.
7. Don't call a number sent in a voicemail or text message. Validate the phone number through the official bank website / Resources and not by using web search engines like Google, Yahoo, Bing, etc.
8. Don't use the same password for multiple accounts.
9. Do not share your password with anybody within the organization or outside.
10. Avoid writing your password close to your desk or nearby as it may fall into the wrong hands.
11. Don't check "remember my password" boxes.
12. Don't enter transaction password on public computers.
13. Do not leave confidential documents and official assets anywhere unattended.
14. Do not enable macros under any circumstances and immediately delete such suspicious emails, asking you to enable macros.
15. Don't discuss something sensitive in public place.
16. Don't plug in personal devices into bank's network

We once again advise the branches to educate the customers on safe and secure use of digital payments and also take all preventive measures to make our Bank safe and secure.

Yours Faithfully,

  
(Vineet Kumar Dudeja)  
Chairman 

---

**HEAD OFFICE**

3<sup>rd</sup> & 4<sup>th</sup> Floor, Suraj Plaza- I, Syajiganj, Vadodara-390005 (Gujarat), INDIA  
Email – [ho@barodagujaratrrb.co.in](mailto:ho@barodagujaratrrb.co.in), website – [www.bqgb.in](http://www.bqgb.in)

**સલામત અને સુરક્ષિત ઇલેક્ટ્રોનિક બેંકિંગ ચેનલો માટે શું કરવું અને શું કરવું નહીં**

DO's ( શું કરવું )	Don'ts ( શું નહીં કરવું )
ખોવાયેલ / ચોરાયેલ એટીએમ કાર્ડ ને બ્લોક કરવા માટે બેંકના ટોલ ફ્રી નંબર "1800229779 અથવા 9323990644" પર તુરંત જ ખોવાયેલ / ચોરાયેલા એટીએમ કાર્ડની જાણ કરો.	ડેબિટ કાર્ડ નંબર, એક્સપાયરી તારીખ, ઓટીપી જેવી ગુપ્ત માહિતી કોઈપણ માધ્યમથી ક્યારેય કોઈ ને આપશો નહીં.
તમારી પેમેન્ટ એપ્લિકેશન માટે નિયમિત અંતરાલો પર તમારો પાસવર્ડ બદલો	કોઈપણ સંવેદનશીલ માહિતી જેવી કે લોગિન આઈડી, પાસવર્ડ, ડેબિટ કાર્ડ વિગતો વગેરેને કાગળ અથવા મોબાઈલ/કમ્પ્યુટર પર સ્ટોર કરશો નહીં.
તમારી પેમેન્ટ એપ્લિકેશન માટે આસાની થી ઉકેલી ન શકાય તેવા પાસવર્ડનો ઉપયોગ કરો.	પ્રાપ્તકર્તા ની માન્યતા વિના રકમ ટ્રાન્સફર અથવા ચુકવણી કરવાની વિનંતિ નો સ્વીકાર ક્યારેય કરશો નહીં, કારણ કે એકવાર ટ્રાન્સફર કરેલ રકમ ફી મેળવી શકાતી નથી
પાસવર્ડ દ્વારા મોબાઈલ ફોનને સુરક્ષિત કરો	સોશિયલ નેટવર્કિંગ સાઈટ્સ / ઇમેઈલ્સ પર અજાણ્યા સ્ત્રોતોની એમ્બેડેડ કરેલી લિંક્સ પર ક્યારેય ક્લિક કરશો નહીં
ઇન્ટરનેટ બેંકિંગ સુવિધા માટે બેંકની વેબસાઈટ માં લોગ ઇન કરતી વખતે 'https' જુઓ અને વેબસાઈટ ના એડ્રેસની ચકાસણી કરો	બેંક સાથે નો સંપર્ક તૂટે નહિ તેના માટે તમારૂં સરનામું, મોબાઈલ નંબર વગેરે બદલે તો તેની જાણ તુરંત જ બેંક ને કરો
એસએમએસ દ્વારા પ્રાપ્ત ટ્રાન્ઝેક્શન ચેતવણીને ચકાસી લો અને અનધિકૃત ટ્રાન્ઝેક્શનની જાણ તુરંત જ બેંક ને કરો	કોઈપણ શંકાસ્પદ એપ્લિકેશનને ક્યારેય ડાઉનલોડ કરશો નહીં અથવા એપ્લિકેશન કોડ કોઈપણ ને આપશો નહીં.

**HEAD OFFICE**3<sup>rd</sup> & 4<sup>th</sup> Floor, Suraj Plaza- 1, Syajiganj, Vadodara-390005 (Gujarat), INDIAEmail – [ho@barodagujaratrrb.co.in](mailto:ho@barodagujaratrrb.co.in), website – [www.bggb.in](http://www.bggb.in)