TEXTILE TRADERS CO-OP. BANK LTD.

સાઈબર સિક્યુરીટી & સાઈબર ક્રાઈમ
કસ્ટમર અવેરનેસ અભિયાન

સાઈબર-સિક્યુરીટી અંગેની થોડી સાવધાની અટકાવશે આપની આર્થિક મોટી હાની...

૬, વસંત વિહાર સોસાયટી, મીઠાખળી સીક્ષ લાઈન રોડ પાસે,

નવરંગપુરા, અમદાવાદ-૩૮૦ ૦૦૯.

ફોનઃ ૦૭૯-૨૬૪૩૦૫૪૫, ૨૬૪૩૪૨૨૩

headoffice@ttcbank.co.in https://ttcbl.com

ફાઈનાન્સીયલ ફ્રોડ / ફેક કૉલ / સોશીયલ મિડીયા ફ્રોડ

- તમારા ખાતા નંબર, ડેબિટ કાર્ડ કે અન્ય કોઈપણ અંગત માહિતી ક્યારેય કોઈપણ બેંક માંગતી નથી. આથી આવી કોઈપણ માહિતી અન્યને આપશો નહીં.
- કોઈ અજાણ્યા મેઈલ / SMS પર આવેલ લીંક પર ક્લીક કરશો નહીં. તે તમારા મોબાઈલ તથા કોમ્પ્યુટરમાં માલવેર વાઈરસ ઈન્સર્ટ કરાવી તમારી માહિતી ચોરી કરશે અને તેનો ગેરઉપયોગ કરી શકે છે.
- SMS કે મેઈલમાં કેશબેક ઓફર્સ, ડિસ્કાઉન્ટ ઓફર, રીવોર્ડ પોઈન્ટ વગેરે આપવા માટે મોકલેલ લીંક પર ક્લીક કરશો નહીં કે ફોન પર માહિતી આપશો નહીં.
- https:\\ થી ચાલુ થતી એડ્રેસવાળી સાઈટ પર જ બેંકીંગ વ્યવહાર કરવો.
- ઓનલાઈન શોપીંગ વેબસાઈટ પર બેંકની કોઈપણ જાતની માહિતી કે કાર્ડ ડીટેલ સેવ કરશો નહીં.
- KYC પૂર્ણ કરવાના બહાને જો કોઈ તમારી બેંકની માહિતી માગે તો આપશો નહીં.
- UPI (Gpay, PhonePay, PayTm) માં હંમેશાં Payment મોકલવા માટે UPI PIN ની જરૂર પડે છે. જ્યારે Payment મેળવવા માટે UPI PIN, OTP Number કે QR Code સ્કેન કરવાની જરૂર પડતી નથી.
- તમારો UPI PIN, Debitcard PIN, Phone Password, Social Media APP Password સમયાંતરે બદલતા રહો.
- Google પર કોઈપણ બેંકનો ટોલ ફ્રી નંબર સર્ચ કરવો નહીં. તેના માટે જે તે બેંકની વેબસાઈટનો જ ઉપયોગ કરવો.
- કોઈપણ લોભામણી સ્કીમ, લોન, ઈન્સ્યોરન્સ, ફંડ ટ્રાન્સફર કરવા માટે રીમોટ એપ જેવી કે Team Viewer, Any Desk, Quick Support, Log Me જેવી એપ ડાઉનલોડ કરવાનું કહે તો કરશો નહીં. આ એપની પરવાનગી તમારા મોબાઈલમાં આપશો નહીં.
- બેંકની Application હંમેશાં Google તથા Apple Play Store પરથી ડાઉનલોડ કરવી.
- Social Media માં અજાણ્યા વ્યક્તિને ક્યારેય મિત્ર બનાવશો નહીં.
- Social Media માં હંમેશાં Privacy Setting Enable, Profile Lock રાખો.
- પબ્લીક WIFI પર મોબાઈલ / નેટબેંકીંગનો ઉપયોગ કરશો નહીં કે બેંકને લગતા કોઈપણ વ્યવહાર કરશો નહીં.
- પબ્લીક પ્લેસ પર ચાર્જીંગ પોઈન્ટ પર મોબાઈલ / લેપટોપ ચાર્જ કરવાનું ટાળો.
- Sova Malware જે બેંકની Application ને હેક કરી, તેની બધી માહિતી ચોરી લે છે. તો હંમેશાં Mobile APP ને Update રાખવી તથા Anti Virus Install રાખવો તથા વખતો વખત અપડેટ કરવો.

BE ALERT

ATM કમ ડેબીટકાર્ડના સુરક્ષિત ઉપયોગ માટે

BE SAFE

આમ કરવું જોઈએ

૧) ડેબીટ કાર્ડ મળ્યા બાદ તુરંત જ કાર્ડની પાછળ આવેલ સફેદ પટ્ટી પર પોતાના હસ્તાક્ષર જરૂરથી કરવા.

૨) તમારો પીન (નંબર) તથા OTP ખાનગી રાખશો.

૩) ATM માં પીન નંબર દાખલ કરતા હોવ ત્યારે કોઈ તે જોતું નથી તેનું ધ્યાન રાખો.

૪) આપના ATM તથા POS ટ્રાન્ઝેક્શનનો SMS એલર્ટ મેળવવા આપનો મોબાઈલ નંબર આપની શાખામાં રજીસ્ટર કરાવવો જરૂરી છે.

૫) જો આપના કાર્ડનો દુરુપયોગ થયેલો જણાય તો તરત જ બેંકને જાણ કરો.

૬) તમારું કાર્ડ સલામત જગ્યાએ મુકો. અથવા કાર્ડ ખોવાઈ જાય તો તેની જાણ તુરંત બેંકને કરો.

૭) Debit કાર્ડમાં આવતી ચીપને નુકશાન ન થાય તેની કાળજી રાખો.

૮) ATM નો ઉપયોગ કરતા પહેલાં આજુબાજુ કોઈ શંકાસ્પદ વ્યક્તિ નથી તેની ખાતરી કરો. જો કોઈ શંકાસ્પદ વ્યક્તિ લાગે તો સિક્યુરીટી ગાર્ડને કહીને તેને દૂર કરાવો અથવા આ સંજોગોમાં ATM નો ઉપયોગ કરવો નહીં.

૯) ATM છોડતા પહેલાં તમારું કાર્ડ, રોકડ તથા રીસીપ્ટ લેવાનું ભૂલશો નહીં. રોકડને વ્યવસ્થિત પાકીટ કે ખીસ્સામાં મૂકીને પછી જ ATM ની બહાર નીકળવું.

૧૦) ATM માં ટ્રાન્ઝેક્શન થયા બાદ Welcome Screen દેખાય ત્યારબાદ જ ATM છોડવું.

૧૧) તમારી પાસબુકની એન્ટ્રીઓ વખતોવખત ચકાસતા રહો જેથી કોઈ ખોટો વ્યવહાર થયો હોય તો તુરંત ધ્યાન ઉપર આવે.

૧૨) ખરીદી કરતી વખતે કાર્ડ તમારી હાજરીમાં જ POS મશીનમાં ઉપયોગ થાય તેનું ધ્યાન રાખો.

આમ ના કરવું જોઈએ

૧) Debit Card નો પીન નંબર કાર્ડ ઉપર લખવો નહીં.

૨) Debit Card નો પીન નંબર તથા OTP કોઈપણ વ્યક્તિ જેવી કે, પોતાના નજીકના સગા, મિત્ર કે બેંકના સ્ટાફને પણ આપવો નહીં.

૩) Debit Card નો પીન નંબર ક્યારેય બીજા જાણી શકે તેવો રાખવો નહીં. દા.ત.: પોતાનો જન્મદિવસ કે લગ્નતિથિ, ટેલિફોન નંબર, વાહનનો નંબર વગેરે.

૪) કાર્ડ ટ્રાન્ઝેક્શન કર્યા પછી કાર્ડ ATM માં જ ભુલાય ન જાય તેનું ધ્યાન રાખવું.

૫) કાર્ડ ક્યારેય પોતાની નજરથી અલગ તેમજ બીજા તેનો દુરુપયોગ કરી શકે તેમ રાખવું નહીં. જેમ કે, કારમાં, હોટેલના રૂમમાં, તમારા ઓફિસમાં, કામ કરવાની જગ્યાએ તથા શોપીંગ મોલમાં વગેરે.

૬) ઇ-મેઇલ ઉપર કે ફોન ઉપર બેંકની વ્યક્તિ તરીકે પણ કોઈ Debit કાર્ડ નંબર, એકાઉન્ટ નંબર, પીન કે OTP માંગે તો પણ આપવો નહીં. બેંક આવી કોઈ માહિતી ક્યારેય પણ આપની પાસેથી માંગશે નહીં.

૭) જો કોઈ ATM યોગ્ય ન લાગતું હોય કે ATM પહેલાં કરતાં અલગ લાગતું હોય કે ATM માં કાર્ડ દાખલ કરવાની જગ્યાએ કોઈ વધારાનું સાધન લગાવેલ હોય ત્યારે તે ATM નો ઉપયોગ કરવો નહીં.

૮) ATM માં કોઈપણ અજાણી વ્યક્તિ કે ચોકીદારની મદદ લેવાનું ટાળો.

સાયબર ક્રાઈમ થવા પાછળના મુખ્ય કારણો

ડર

નાગરિકો / ગ્રાહકોને વિડીયો કોલીંગ / અહિત વિડીયો બનાવી અને તે વિડીયો સોશીયલ મિડીયા પર શેર કરવાનો ડર બતાવી, બ્લેકમેલ કરી છેતરપીંડીનો ભોગ બનાવવામાં આવે છે.

લાલચ

નાગરિકો/ગ્રાહકો ઘણી વખત ઈનામ, લોટરી, ડિસ્કાઉન્ટ જેવી લોભામણી ઓફરની જાળમાં આવીને મોબાઈલમાં આવતા મેસેજ અથવા લીંક પર ક્લીક કરીને આર્થિક છેતરપીંડીનો ભોગ બનતા હોય છે.

બેદરકારી

નાગરિકો/ગ્રાહકો ઘણી વખત મેસેજ કે ઈ-મેઈલની ખરાઈ કર્યા વગર તુરંત જ એકાઉન્ટ / કાર્ડ / પીન તેમજ ઓ.ટી.પી. નંબર આપીને આર્થિક છેતરપીંડીનો ભોગ બનતા હોય છે.

ટેક્ષટાઈલ ટ્રેડર્સ કો.ઓપ. બેન્ક વિશે વધારે માહિતી મેળવવા તથા વર્તમાન સમયમાં થતાં CYBER FRAUDને લગતી માહિતી જાણવા અને CYBER FRAUDથી સતર્ક રહેવા નીચે મુજબનાં Pageને Facebookમાં Like અને Follow કરો.

TEXTILE TRADERS CO-OP. BANK LTD.

RBI Says

Gujarat Cyber Crime Cell

આપની સુરક્ષા, આપની સમજદારીમાં જ છે.

સાયબર ક્રાઈમની ફરિયાદ માટે

હેલ્પલાઈન નંબર : ૧૯૩૦

www.cybercrime.gov.in