મોબાઇલ વોલેટ

શું કરવું:

- હંમેશા અધિકૃત વોલેટ એપ્સની ખરાઈ કરો અને ઈન્સ્ટોલ કરો
- તમારો ફોન પિન દ્વારા સુરક્ષિત રાખો
- ટ્રાન્જેક્શન્સ પહેલા લાભાર્થીનો મોબાઇલ નંબર સાચો હોવાની ખાતરી કરી લો

શું ન કરવું:

- તમામ વોલેટ્સ માટે એકસરખો પાસવર્ડ ન રાખો
- પેમેન્ટ કરવા માટે ઓપન વાઇ-ફાઇ અથવા ચકાસ્યા વિનાના ડિવાઇસોનો ઉપયોગ ન કરા
- અવિશ્વસનિય QR કોડ્સ સ્કેન ન કરો

જાગૃતિ અભિયાન ભાગીદારો

નાબાર્ડ

NPCI

airtel Payments Bank

AXIS BANK

mastercard

paytm payments bank

PayPal

VISA

Follow us

dsci_connect

dsci.connect

dsci-security-council-of-India

Digital India
Power To Empower

Ministry of Electronics and Information Technology
Government of India

DIGITAL PAYMENT
suraksha

A Joint Initiative of

DSCI | Google

PROMOTING DATA PROTECTION

"Digital money will empower the poor"

- Narendra Modi
Prime Minister

ડિજિટલ પેમેન્ટ

#SaralBhiSecureBhi

આ હેન્ડી બૂકલેટની મદદથી ડિજિટલ પેમેન્ટ્સ વખતે શું કરવું અને શું ન કરવું એ વિષે માહિતીસભર રહો

આ સ્કેન કરો

www.dsci.in/digital-payment-suraksha

ઓનલાઇન અને મોબાઇલ બેન્કિંગ

શું કરવું:

- પેમેન્ટ માટે માત્ર ચકાસેલા અને વિશ્વસનિય બ્રાઉઝરો અને HTTPS દ્વારા સુરક્ષિત વેબસાઇટોનો ઉપયોગ કરો
- અવારનવાર પાસવર્ડ્સ બદલતા રહો અને એની સાથે ચેડા થાય ત્યારે તરત જ બદલો
- તમારી પેમેન્ટ ટ્રાન્જેક્શન એપ્લિકેશનો (બેંકો/પેમેન્ટ બેંકો/વોલેટો) લેટેસ્ટ વર્ઝનથી અપડેટ રાખો

શું ન કરવું:

- ફોનમાં લોગઇન ક્રેડેન્શિયલ્સ ક્યારેય સાચવી ન રાખો; અવિશ્વશનિય કિઓસ્ક્સ પર પણ ક્રેડેન્શિયલ્સ એંટર ન કરો
- જાહેર ડિવાઇસો અને અસુરક્ષિત/ઓપન નેટવર્ક્સ મારફતે ટ્રાન્જેક્શન કરવાનું ટાળો
- કોઈપણ વ્યક્તિ સાથે તમારો મોબાઇલ બેન્કિંગ પિન શેર ન કરો

યુએસએસડી પેમેન્ટ

શું કરવું:

- કોઈપણ ટ્રાન્જેક્શન કરતા પહેલા મોબાઇલ મની આઇડેન્ટિફાયર અને મોબાઇલ નંબરની હંમેશા ખરાઈ કરો
- તમારો M-પિન નિયમિત સમયાંતરે અવશ્ય બદલો
- આવી રહેલી USSD રીક્વેસ્ટ્સ બાબતે સાવધ રહો

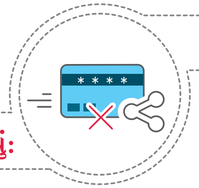
શું ન કરવું:

- તમારો M-પિન કોઈપણ વ્યક્તિ સાથે ક્યારેય શેર ન કરો
- તમારો M-પિન ક્યારેય ક્યાંય લખો નહીં
- તમારો OTP કોઈપણ વ્યક્તિ સાથે શેર ન કરો

કેડિટ અને ડેબિટ કાર્ડ

શું કરવું:

- તમારા કાર્ડનો ઉપયોગ થતો હોય તે વખતે હંમેશા તેના પર નજર રાખો અને તરત જ પાછું લઈ લો
- હંમેશા ચકાસો કે ટ્રાન્જેક્શન એસએમએસ વિગતો અને વાસ્તવિક ટ્રાન્જેક્શન વચ્ચે કંઈ ફરક ન હોય
- રસીદો અને સ્ટેટમેન્ટ્સનો સુરક્ષિત રીતે નિકાલ કરો



શું ન કરવું:

- વેપારીઓને ક્યારેય તમારા કાર્ડની વિગતો સ્ટોર કરવા ન દો
- કોઈપણ વ્યક્તિને CVV અને પિન ન આપો
- કોઈ પાસે તમારા કેડિટ અથવા ડેબિટ કાર્ડ છોડીને ન જાવ

યુનિફાઈડ પેમેન્ટ ઇન્ટરફેસ અને BHIM

શું કરવું:

- વેપારીને પેમેન્ટ કરતા પહેલા પેમેન્ટ કલેક્ટ રીક્વેસ્ટ વિગત ચકાસો
- UPI-આધારિત એપ્સ અપડેટેડ હોવાની હંમેશા તકેદારી રાખો
- ઓળખીતા લાભાર્થીઓને જ રૂપિયા ટ્રાન્સફર કરો છો, એ બાબત સુનિશ્ચિત કરો

શું ન કરવું:

- તમારો UPI M-પિન ક્યારેય શેર ન કરો કે લખીને ન રાખો
- UPI/BHIM ટ્રાન્જેક્શન્સ માટે જેલબ્રોકન ડીવાઇસોનો ઉપયોગ ટાળો
- પ્રાપ્તકર્તાની ખરાઈ કર્યા વિના ક્યારેય રૂપિયા ટ્રાન્સફર ન કરો

આધાર સાથેની પેમેન્ટ સિસ્ટમ

શું કરવું:

- રૂપિયા ટ્રાન્સફર કરતા પહેલા હંમેશા આધાર નંબર ચકાસી લો
- ટ્રાન્જેક્શન કરવું હોય તો માત્ર POS અને બાયોમેટ્રિક ડેટા કેપ્ચર ડિવાઇસ પર આધાર આઈડીનો ઉપયોગ કરો
- ડિવાઇસ (POS અને બાયોમેટ્રિક ડેટા કેપ્ચર ડિવાઇસ મશિન) સાથે છેડછાડ કરવામાં નથી આવી અને માત્ર પ્રમાણિત ડિવાઇસોનો જ ઉપયોગ થઈ રહ્યો હોવાની ખાત્રી કરો

શું ન કરવું:

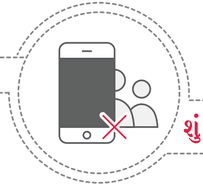
- વેપારીઓને તમારા બાયોમેટ્રિક્સ અને કાર્ડની વિગતો ક્યારેય સ્ટોર કરવા ન દો
- તમારું AEPS કાર્ડ કોઈપણ જગ્યાએ અને નજરથી દૂર ન જવા દો
- યોગ્ય કારણ વિના તમારી આધાર અને અંગત વિગતો ન આપો

મૂળભૂત આવશ્યકતાઓ

શું કરવું:

- તમારું ડિવાઇસ હંમેશા અપડેટ, લોક અને મજબૂત પાસવર્ડ દ્વારા સુરક્ષિત રાખો
- ટ્રાન્જેક્શન લોગ્સ અને એલર્ટ્સ પર નજર રાખો; શંકાસ્પદ અથવા છેતરપિંડીયુક્ત પ્રયાસો વિષે લાગતા-વળગતા સર્વિસ પોર્વાઇડર્સ અને પોલિસ અધિકારીઓને જાણ કરો
- જો તમારું ડિવાઇસ ખોવાઈ કે ચોરાઈ જાય તો તરત જ તમારું સિમ બ્લોક કરી દો અને જે-તે બેંક-વોલેટ સંસ્થા અને પોલિસ અધિકારીઓને જાણ કરો
- સંવેદનશીલ નાણાકિય માહિતી માગતા અનિચ્છનિય કોલ્સ, મેસેજીસ અને ઇમેઇલ્સથી સાવધાન રહો
- ફાયરવોલ્સ, વાયરસ મેલવેર અને ઇન્ટ્રુઝન-ડિટેક્શન સિસ્ટમ સહિતના થ્રીટ્સ શોધવા અને દૂર કરવા માટેની એપ્લિકેશન્સ ઇન્સ્ટોલ કરેલી અને સક્રિય હોવી જોઈએ
- તમારા ડિવાઇસોમાં માત્ર સારા રીવ્યુઝ ધરાવતી અધિકૃત એપ સ્ટોર્સમાંથી ડાઉનલોડ કરો
- બેંકની વેબસાઇટો પરની લિંકો પરથી એપ્લિકેશન્સની અધિકૃતતાની ચકાસણી કરો

મૂળભૂત આવશ્યકતાઓ



શું ન કરવું:

- એડમિનિસ્ટ્રેટિવ પ્રિવિલેજીસ સાથે ક્યારેય ઈન્ટરનેટ એક્સેસ ન કરો
- SMS અથવા email પર પ્રાપ્ત થતી શંકાસ્પદ લિંક્સ પર ક્લિક ન કરો
- અવિશ્વસનિય અને વણચકાસેલા સ્ત્રોતોમાંથી આવતી એપ્સ ક્યારેય ઈન્સ્ટોલ ન કરો
- મોબાઇલ બેન્કિંગ માટે જેલબ્રોકન અથવા રૂટેડ ડીવાઇસો
- ઓનલાઇન ડિજિટલ પેમેન્ટ્સ માટે અસુરક્ષિત WiFi પોઇંટ્સ સાથે કનેક્ટ ન કરો
- અજાણ્યા સ્ત્રોતો તરફથી આવતા ઇમેઇલ્સ અથવા એટેચમેન્ટ્સ ખોલવા કે ડાઉનલોડ કરવાનું ટાળો
- અજાણ્યા લોકોના હાથમાં ડીવાઇસ ક્યારેય ન આપો
- ડેબિટ કાર્ડ/કેડિટ કાર્ડ/એટીએમ પિન/સીવીવી/એક્સપાયરી ડેટ અથવા પાસવર્ડ્સ માગતા ઇમેઇલ્સ, ફોન કોલ્સ અથવા ટેક્સ્ટ મેસેજીસને જવાબ આપવાનું ટાળો