યુનિફાઈડ પેમેન્ટ ઇન્ટરફેસ અને BHIM

શું કરવું:

- હંમેશા UPI ટ્રાન્ઝેક્શન્સનો રેકોર્ડ રાખો
- એ વાત સુનિશ્ચિત કરો કે કર્મચારીઓ છેતરપિંડીઓ વિષે જાણતા હોય
- છેતરપિંડી થઈ શકે એવી પ્રવૃત્તિઓ, જેમકે પિન શેર કરવો, ખાતા નંબર અને અંગત વિગતો આપવી વગેરે જેવી બાબતોને પ્રોત્સાહન આપવું જોઈએ નહીં

શું ન કરવું:

- બાયોમેટ્રિક્સ અને એમ-પિન વિગતો કોઈપણ પ્રકારે એટલેકે ફિઝિકલ કે ઇલેક્ટ્રોનિક રીતે સ્ટોર કરવી ન જોઈએ
- ગ્રાહકોની માહિતીની સુરક્ષા ક્યારેય ન અવગણો
- ગ્રાહકની વિગતો ખરાઈ કર્યા વિના કલેક્ટ રીક્વેસ્ટ જારી ન કરો

જાગૃતિ અભિયાન ભાગીદારો

Government of Telangana

नाबार्ड

NPCI
भारतीय राष्ट्रीय भुगतान निगम
NATIONAL PAYMENTS CORPORATION OF INDIA

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 PROMOTING DATA PROTECTION | Google

"Digital money will empower the poor"

- Narendra Modi
Prime Minister

ડિજિટલ પેમેન્ટ

#SaralBhiSecureBhi

તમારા ગ્રાહકો તરફથી ડિજિટલ પદ્ધતિએ પેમેન્ટ મેળવતી વખતે આ બુકલેટ તમને શું કરવું અને શું ન કરવું એ ધ્યાનમાં રાખવામાં મદદ કરશે.

www.dsci.in/digital-payment-suraksha

આ સ્કેન કરો

આધાર સાથેની પેમેન્ટ સિસ્ટમ

શું કરવું:

- ડિવાઇસ (POS અને બાયોમેટ્રિક ડેટા કેપ્ચર ડિવાઇસ મશિન) સાથે છેડછાડ કરવામાં નથી આવી અને માત્ર પ્રમાણિત ડિવાઇસોનો જ ઉપયોગ થઈ રહ્યો હોવાની ખાત્રી કરો
- તમારા POS હંમેશા અપગ્રેડ રાખો અને એની સુરક્ષા જાળવી રાખો
- POSની શંકાસ્પદ હિલચાલ વિષે તરત જ રીપોર્ટ કરવાનું સુનિશ્ચિત કરો

શું ન કરવું:

- POS ખુલ્લી કે અસુરક્ષિત જગ્યાઓ પર રાખવાનું ટાળો
- સ્લિપ્સ અને રીપોર્ટ્સમાં સંપૂર્ણ કાર્ડ કે આધારની વિગતો ક્યારેય પ્રિન્ટ ન કરો
- આધાર વિગતો - નંબર, અંગત માહિતી, બાયોમેટ્રિક્સ સ્ટોર કરેલા ન હોવા જોઈએ

મૂળભૂત આવશ્યકતાઓ

શું કરવું:

- પેમેન્ટ્સ સંભાળતા તમારા કર્મચારીઓને થ્રીટ્સ વિષે હંમેશા માહિતગાર રાખો
- હંમેશા સુરક્ષિત અને ભરોસાપાત્ર અને સંપૂર્ણરીતે ચકાસાયેલા પેમેન્ટ ગેટવેઝનો ઉપયોગ કરો
- બેંકની વેબસાઇટો પરની લિંકો પરથી એપ્લિકેશન્સની અધિકૃતતાની ચકાસણી કરો
- ઉપયોગ થઈ રહ્યા હોય એ ડિવાઇસો (POS અને બાયોમેટ્રિક કેપ્ચર મશિન) અપડેટેડ છે અને તેની સાથે છેડછાડ કરવામાં નથી આવી તથા માત્ર પ્રમાણિત ડિવાઇસોનો જ ઉપયોગ થઈ રહ્યો હોવાની ખાત્રી કરો
- ટ્રાન્જેક્શન લોગ્સ અને એલર્ટ્સ પર નજર રાખો; શંકાસ્પદ અથવા છેતરપિંડીયુક્ત પ્રયાસો વિષે લાગતા-વળગતા સર્વિસ પોર્વાઇડર્સ અને પોલિસ અધિકારીઓને જાણ કરો

શું ન કરવું:

- અવિશ્વસનિય અને ચકાસેલી ન હોય તેવા સ્ત્રોતો/એપ સ્ટોર્સમાંથી એપ્સ ક્યારેય ઇન્સ્ટોલ ન કરો
- ડિજિટલ પેમેન્ટ્સ સ્વિકારતી વખતે ક્યારેય અસુરક્ષિત/ઓપન વાઇ-ફાઇ પોઇન્ટ્સનો ઉપયોગ ક્યારેય ન કરો
- પેમેન્ટ ડિવાઇસો ક્યારેય ધ્યાન બહાર ન રાખો અથવા અજાણી વ્યક્તિઓને ન આપો
- ગ્રાહકોની સંવેદનશીલ માહિતી જેવીકે બાયોમેટ્રિક, એમ-પિન, પાસવર્ડ્સ વગેરે કોઈપણ પ્રકારે (ફિઝિકલ/ઇલેક્ટ્રોનિક) ક્યારેય સ્ટોર ન કરો

ઓનલાઇન અને મોબાઇલ બેંકિંગ

શું કરવું:

- હંમેશા સુરક્ષિત અને ભરોસાપાત્ર પેમેન્ટ ગેટવેઝનો ઉપયોગ કરો
- પેમેન્ટ ગેટવે ઈન્ટિગ્રેશન સંપૂર્ણપણે ચકાસેલું છે એની ખાતરી કરો
- ગ્રાહકો ઓનલાઇન અને મોબાઇલ બેંકિંગનો ઉપયોગ કરી શકે છે કે નહીં એ નિયમિત રીતે ચકાસો

શું ન કરવું:

- ગ્રાહકોને તેઓની ઓનલાઇન બેન્કિંગ માહિતીઓ વિષે પૂછવાનું ટાળો
- પેમેન્ટ મોડ્યુલની સુરક્ષાની અવગણના ક્યારેય ન કરો
- છેતરપિંડીના પ્રયત્નો ક્યારેય ન અવગણો અને તરત જ બેન્ક/પેમેન્ટ ગેટવેને જાણ કરો

મોબાઇલ વોલેટ

શું કરવું:

- વોલેટ્સમાંથી પ્રાપ્ત થતા પેમેન્ટ હંમેશા ટેલી કરો અને ટ્રાન્જેક્શન રેફરન્સ નંબરો પર નજર રાખો
- ગ્રાહકો સુરક્ષિત અને સ્ટેટિક QR કોડનો ઉપયોગ કરીને ટ્રાન્જેક્શન કરવા સક્ષમ છે એ નિયમિત રીતે ચકાસતા રહો
- સંવેદનશીલ માહિતી શેર કરતા પહેલા એજન્ટના અધિકૃત આઇડીની હંમેશા ખરાઈ કરી લેવી

શું ન કરવું:

- ગ્રાહકોની સંવેદનશીલ માહિતી કોઈપણ રીતે (ફિઝિકલ/ઇલેક્ટ્રોનિક) સ્ટોર ન કરો
- છેતરપિંડીના પ્રયાસો ક્યારેય ન અવગણો અને લાગતી-વળગતી વોલેટ કંપનીને તરત જ જાણ કરો
- જરૂર ન હોય એવી ગ્રાહકોની માહિતી મેળવવાનું ટાળો

ક્રેડિટ અને ડેબિટ કાર્ડ

શું કરવું:

- ગ્રાહકની દેખરેખ હેઠળ જ કાર્ડ ટ્રાન્જેક્શન કરો
- તમારા POS હંમેશા અપગ્રેડ રાખો અને એની સુરક્ષા જાળવી રાખો
- POS ડિવાઇસો સાથે છેડછાડ નથી થઈ અને માત્ર પ્રમાણિત ડિવાઇસો નો જ ઉપયોગ થઈ રહ્યો હોવાની ખાત્રી કરો

શું ન કરવું:

- POS ડિવાઇસો નજરથી દૂર/દેખરેખથી દૂર ન જાય અને અનધિકૃત લોકો તેનો ઉપયોગ ન કરે એની તકેદારી રાખો
- કાર્ડના CVV અને પિન ક્યારેય સ્ટોર ન કરો
- સંપૂર્ણપણે જરૂરી ન હોય ત્યાં સુધી ગ્રાહકોના કાર્ડની વિગતો સ્ટોર ન કરો