સતર્ક રહો અને સુરક્ષિત બેન્ક વ્યવહાર કરો

બેન્કિંગ ધ્યાન સે

સાથે

AXIS BANK

એક્સિસ બેન્ક દ્વારા ગ્રાહક સેવા પહેલ

સ્વીકૃતિ

આ દસ્તાવેજ આરબીઆઈ લોકપાલ (મુંબઈ – 2) મહારાષ્ટ્ર, ગોવાનાં કાર્યાલય અને આ વિષયી બાબત પર અમારા અમુક ઈન–હાઉસ રિસર્ચ દ્વારા જારી 'અ બુકલેટ ઓન મોડસ ઓપરેન્ડી ઓફ ફાઈનાન્શિયલ ફ્રોડસ્ટર્સ' (અર્થાત, નાણાકીય ઠગોની પદ્ધતિ પર પુસ્તિકા) પરથી ઈનપુટ્સને આધારે તૈયાર કરવામાં આવ્યો છે.

પ્રસ્તાવના

બેન્ક વ્યવહારની પ્રણાલીએ સહજ અને ઝડપથી નાણાકીય જરૂરતો પરિપૂર્ણ કરવા ગ્રાહકો માટે નવાં દ્વાર ખોલી નાખ્યાં છે. વર્તમાન સ્થિતિ ઓછામાં ઓછા પ્રત્યક્ષ અને સામાજિક સંપર્ક સાથે શક્ય હોય ત્યાં સુધી ડિજિટલ અપનાવવા માટે આપણને પ્રોત્સાહન આપી રહી છે.

ડિજિટલ બેન્કિંગની વધતી સુવિધાનો આપણે લાભ લઈ રહ્યા છીએ ત્યારે બીજી બાજુ સાઈબર ગુના અને બેન્કિંગ છેતરપિંડી પણ વધી છે. મોટે ભાગે ગ્રાહકોને ઊંઘતાં ઝડપી લેવાય છે અને જો તેઓ સાવધાન નહીં રહે તો નાણાકીય નુકસાન ભોગવવું પડી શકે છે.

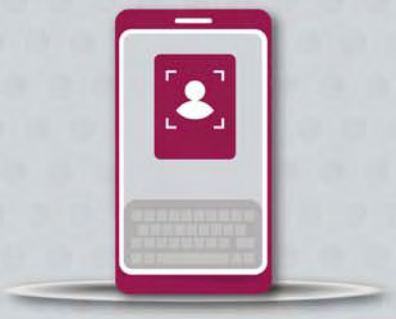
એક્સિસ બેન્કમાં અમે તમારી કાળજી રાખીએ છીએ અને સમયાંતરે ઉપયોગી માહિતી આપીને તમારા હિતનું રક્ષણ કરવા માટે તમને મદદરૂપ થવા સતત પગલાં લઈએ છીએ.

આ દસ્તાવેજ આજે પ્રવર્તમાન શંકાસ્પદ અને છેતરપિંડીની પ્રવૃત્તિઓ સાથે તમને સતર્ક અને પરિચિત કરવા માટે અમારી પહેલ છે. અમે આવી પ્રવૃત્તિઓને કઈ રીતે ઓળખવી, તમારે કેવી સાવચેતીઓ રાખવી જોઈએ અને તે વિશે જાણકારી કઈ રીતે આપવી જોઈએ તે વિશે સમજવામાં તમને મદદરૂપ થવા અમુક પ્રચલિત છેતરપિંડીની પ્રવૃત્તિઓનું સંકલન કર્યું છે. સાવચેત રહેવાથી નાણાકીય નુકસાનનો ભોગ બનવાની અને તે ઉદભવવાની શક્યતા ઓછામાં ઓછી કરવામાં તમને મદદ થશે.

અમને વિશ્વાસ છે કે તમને આ માહિતી ઉપયોગી જણાશે અને તમે બેન્કિંગ ધ્યાન સે કરો ત્યારે સુરક્ષિત અને સહજ બેન્કિંગ અનુભવ થશે.

સુરક્ષિત રહો!

અહીં અમુક સામાન્ય સાવચેતીનાં પગલાં અને ઉત્તમ વ્યવહારોની માહિતી આપી છેઃ



આ કરવાનું ટાળો

- અસંરક્ષિત વેબસાઈટ્સની વિઝિટ્સ કરવી અથવા અજ્ઞાત બ્રાઉઝર્સનો ઉપયોગ કરવો
- પબ્લિક ડિવાઈસીસ પર પાસવર્ડસ સેવ કરવા
- જાહેર અથવા ફ્રી નેટવર્કસ પરથી નાણાકીય/ગોપનીય ઈમેઈલને એક્સેસ મેળવવો
- શંકાસ્પદ દેખીતા પોપ અપ્સ, અજ્ઞાત સ્રોતોમાંથી લિંક્સ અને ઈમેઈલ્સ પર ક્લિક કરવું
- ઈમેઈલ્સ અથવા અજ્ઞાત વેબસાઈટ્સ પરથી સંરક્ષિત ક્રિડેન્શિયલ્સ અથવા પાસવર્ડસનો સંગ્રહ કરવો
- સોશિયલ મિડિયા પર અજ્ઞાત વ્યક્તિઓને ગોપનીય માહિતી આપવી
- બેન્કિંગ અને અન્ય લેણદેણ માટે એકસમાન પાસવર્ડસનો ઉપયોગ કરવો
- અજ્ઞાત એપ્લિકેશન્સ અથવા સોફ્ટવેર ઈન્સ્ટોલ કરવું
- તમારો મોબાઈલ અથવા અન્ય ઈલેક્ટ્રોનિક ડિવાઈસીસ અથવા એપ્સ અનલોક છોડી દેવાં

આ કરવાથી બચો

- તમારો પિન (પર્સનલ આઈડેન્ટિફિકેશન નંબર), પાસવર્ડ, ક્રેડિટ કે ડેબિટ કાર્ડ નંબરો, સીવીવી, ચેકબુકની કોપીઓ, કેવાયસી વિગતો કોઈને પણ નહીં આપવું જોઈએ
- અજ્ઞાત ડિવાઈસીસ પર સંવેદનશીલ અથવા ગોપનીય માહિતીનો સંગ્રહ નહીં કરવો જોઈએ

આ હંમેશાં ધ્યાન રાખો

- તમારા ફોનનું મજબૂત સ્ક્રીન પાસવર્ડ સાથે રક્ષણ કરો
- લાગુ/ઉપલબ્ધ હોય ત્યાં ટુ–ફેક્ટર ઓથેન્ટિફિકેશનનો ઉપયોગ કરો
- ઉપયોગ પછી તુરંત ઈન્ટરનેટ બેન્કિંગ સેશનમાંથી લોગઆઉટ કરો
- એનેબલ અથવા ડિઝેબલ ફીચરનો ઉપયોગ કરો અને તમારા કાર્ડ પર અથવા તમારા ઉપયોગને આધારે અકાઉન્ટ આધારિત લેણદેણ મર્યાદિત સ્થાપિત કરો
- પેડલોક અથવા https જેવાં સંરક્ષિત ચિહ્નો જોઈને વેબસાઈટની સલામતી વેરિફાઈ કરો
- ઓનલાઈન પેમેન્ટ્સ માટે સંરક્ષિત પેમેન્ટ ગેટવેઝનો ઉપયોગ કરો
- આલ્ફાન્યુમેરિક અને સ્પેશિયલ કેરેક્ટર્સનું સંયોજન હોય તેવા મજબૂત પાસવર્ડસ રાખો અને નિયમિત રીતે તે બદલી કરો
- પબ્લિક ડિવાઈસીસ પર વર્ચ્યુઅલ કીબોર્ડનો ઉપયોગ કરો, કારણ કે કીસ્ટ્રોક્સ પણ બાંધછોડ થઈ શકતાં ડિવાઈસીસ, કીબોર્ડ વગેરે થકી કેપ્ચર કરી શકાય છે
- તમારાં ડિવાઈસીસ પર એન્ટીવાઈરસ અને એન્ટીસ્પાયવેર્સ ઈન્સ્ટોલ કરો, તેમને અપટુડેટ રાખો અને ઉપલબ્ધ થાય ત્યાં અપડેટ્સ ઈન્સ્ટોલ કરો
- ઉપયોગ પૂર્વે કોઈ પણ યુએસબી ડ્રાઈવ્ઝ/સ્ટોરેજ ડિવાઈસીસ સ્કેન કરો
- તમારા મોબાઈલ એપ્સને પાસવર્ડથી સુરક્ષિત રાખો અથવા મોબાઈલ ફોન્સમાં છૂપા સ્પેસ ફીચરનો ઉપયોગ કરીને નોર્મલ વ્યુથી તેને કન્સલ કરો

#BankingDhyaanSe

ઓનલાઈન/વેબસાઈટ છેતરપિંડી વિશે (1)

મોડસ ઓપરેન્ડી
તમે સાવચેત અને સુરક્ષિત કઈ રીતે રહી શકો છો?

ઓનલાઈન ફિશિંગ

આ કઈ રીતે કરાય છે

- ઠગો એવી વેબસાઈટ તૈયાર કરે છે જે બેન્કની અસલી વેબસાઈટ હોય તેવું જ દેખાય છે
- આ વેબસાઈટની લિંક્સ એસએમએસ, સોશિયલ મિડિયા, ઈમેઈલ વગેરે થકી વિતરણ કરવામાં આવે છે
- આ લિંક્સ અસલી વેબસાઈટ જેવી દેખાય તે માટે માસ્ક્ડ કરાય છે અને લિંક પર એક નજર કરતાં જ અને વિગતવાર યુઆરએલ તપાસ નહીં કરતાં તમારી વિશ્વસનીય કે સંવેદનશીલ અને ગોપનીય માહિતી એન્ટર કરવા માટે તમને આકર્ષિત કરે છે
- તમે આ વેબસાઈટ્સ પર તમારી ક્રિડેન્શિયલ્સ એન્ટર કરવા પર તે ઠગો દ્વારા કેપ્ચર અને દુરુપયોગ કરવામાં આવે છે

સુરક્ષાની ટિપ્સ

- જો અસલી દેખાતી હોય તો પણ અજ્ઞાત લિંક્સ ટાળો
- નાણાકીય ક્રિડેન્શિયલ્સ એન્ટર કરવા પૂર્વે વેબસાઈટની વિગતો વેરિફાઈ કરો

ઓનલાઈન છેતરપિંડી

આ કઈ રીતે કરવામાં આવે છે

- ઠગો ઓનલાઈન, ઈકોમર્સ મંચો પર કાયદેસર ખરીદદારો/વિક્રેતાઓ હોવાનો દેખાડો કરે છે
- તેઓ તમારી પ્રોડક્ટમાં રસ બતાવે છે અને વ્યાપક ડિસ્કાઉન્ટ્સ અથવા ઈન્સેન્ટિવ્ઝ આપીને તેમની પાસેથી ખરીદી કરવા તમને આકર્ષિત કરે છે
- પેમેન્ટ કરવાને બદલે તેઓ તમારા બેન્ક અકાઉન્ટમાંથી પૈસા ઉપાડવા માટે યુપીઆઈ 'રિક્વેસ્ટ મની' વિકલ્પ પૂર્ણ કરવા લલચાવે છે

સુરક્ષાની ટિપ્સ

- ઓનલાઈન પ્રોડક્ટો માટે નાણાકીય લેણદેણ કરો ત્યારે કાળજી રાખો
- તમને નાણાં પ્રાપ્ત કરવા માટે તમારો પિન અથવા પાસવર્ડ એન્ટર કરવા માટે ક્યારેય પૂછવામાં નહીં આવશે

#BankingDhyaanSe

ઓનલાઈન/વેબસાઈટ છેતરપિંડી વિશે (2)

મોડસ ઓપરેન્ડી
તમે સાવચેત અને સુરક્ષિત કઈ રીતે રહી શકો છો?

બોગસ સર્ચ એન્જિન પરિણામો

તે કઈ રીતે કરવામાં આવે છે

- ઠગો કંપનીઓના કસ્ટમર કેર કોઓર્ડિનેટ્સ સુધારે છે અને સોશિયલ મિડિયા મંચો પર સર્ચ રિઝલ્ટ્સની ટોચ પર તેમના નકલી નંબર પુશ કરવા સર્ચ એન્જિન ઓપ્ટિમાઈઝેશન (એસઈઓ)નો ઉપયોગ કરે છે
- તમારી બેન્ક અથવા અન્ય નાણાકીય માહિતી/એન્ટિટીઝની કસ્ટમર કેર સંપર્ક વિગતો માટે ઓનલાઈન સર્ચ કરો ત્યારે તમે અકસ્માતે એવા અનવેરિફાઈડ/નકલી નંબરોના સંપર્કમાં આવી શકો છો જે અસલી હોવાનું દેખાય છે
- તમે અંગત અથવા ગોપનીય અને નાણાકીય ક્રિડેન્શિયલ્સ આપીને ઠગાઈનો ભોગ બની શકો છો

સુરક્ષાની ટિપ્સ

- સર્ચ એન્જિન પર કસ્ટમર કેર સંપર્ક વિગતોની સર્ચ કરવાનું ટાળો, કારણ કે તેમાં ઠગો દ્વારા પીડિતોને લલચાવવા માટે ચેડાં કરવામાં આવ્યાં હોઈ શકે છે
- હંમેશાં અસલી સંપર્ક વિગતો માટે બેન્કો/કંપનીઓની વિધિસર વેબસાઈટ્સ જુઓ

આ કઈ રીતે કરવામાં આવે છે

આ કઈ રીતે કરવામાં આવે છે

- સ્ક્રીન શેરિંગ એપ્સ ડાઉનલોડ કરવા માટે તમને આકર્ષિત કરીને પછી તમારાં બેન્કિંગ અને પેમેન્ટ એપ્સનો ઉપયોગ કરીને પેમેન્ટ્સ કરવા ઠગો તમારા લેપટોપ/મોબાઈલ ડિવાઈસીસ પર તમારો અંગત ડેટા અને નાણાકીય ક્રિડેન્શિયલ્સને પહોંચ મેળવી શકે છે

સુરક્ષાની ટિપ્સ

- કોઈ પણ અજ્ઞાત વ્યક્તિઓ દ્વારા સૂચિત સ્ક્રીન શેરિંગ એપ્સ ડાઉનલોડ નહીં કરો
- કોઈ પણ બેન્કિંગ અથવા નાણાકીય એપ કે વેબસાઈટમાં લોગઈન કરવા પૂર્વે કોઈ પણ સ્ક્રીન શેરિંગ એપ્લિકેશન ડિએક્ટિવેટ કરવાની ખાતરી રાખો

ઓન કોલ/મોબાઈલ છેતરપિંડી વિશે (1)

મોડસ ઓપરેન્ડી
તમે સાવચેત અને સુરક્ષિત કઈ રીતે રહી શકો છો?

વિશિંગ કોલ્સ

આ કઈ રીતે કરવામાં આવે છે

- ઠગો અમુક વાર તમારી બેન્કનો ટોલ ફ્રી અથવા કસ્ટમર કેર નંબર સ્પૂફ કરીને બેન્કિંગ એક્ઝિક્યુટિવ વગેરે તરીકે પોતાની ઓળખ આપીને ટેલિફોન કલ/સોશિયલ મિડિયા થકી ગ્રાહકોને સંપર્ક કરી શકે છે
- કોલર સેવાઓ તુરંત બંધ કરાશે, કેવાયસીનું પાલન કરાયું નથી, અકાઉન્ટ/કાર્ડ બંધ કરાશે વગેરે જેવાં વિવિધ તાકીદનાં કારણો આપીને તેમની ગોપનીય વિગતો અથવા ઓટીપી આપવા માટે ગ્રાહકોને સમજાવવા દબાણ અને પ્રયાસ કરે છે
- તેઓ તમારા અકાઉન્ટમાં છેતરપિંડીની પ્રવૃત્તિઓ પાર પાડવા માટે તેમની ક્રિડેન્શિયલ્સનો દુરુપયોગ કરી શકે છે

સુરક્ષાની ટિપ્સ

- બેન્ક/કોઈ પણ જેન્યુઇન એન્ટિટી ક્યારેય યુઝરનેમ, પાસવર્ડ, કાર્ડની વિગતો, પિન, સીવીવી, ઓટીપી વગેરે જેવી ગોપનીય માહિતી આપવા માટે ક્યારેય પૂછી નહીં શકે

મોબાઈલ એપ છેતરપિંડી

આ કઈ રીતે કરવામાં આવે છે

- તમને તમારા મોબાઈલ, લેપટોપ અથવા ડેસ્કટોપ પર અનવેરિફાઈડ એપ ડાઉનલોડ કરવા માટે લલચાવવામાં આવે છે
- આ એપ્સની લિંક્સ એસએમએસ, સોશિયલ મિડિયા મંચો વગેરે થકી શેર અને પ્રમોટ કરાય છે
- તે બદઇરાદાભર્યાં એપ્લિકેશન્સ હોય છે, જે ઠગોને તમારા ડિવાઇસને સંપૂર્ણ પહોંચ મેળવવામાં મદદ કરે છે

સુરક્ષાની ટિપ્સ

- અનવેરિફાઈડ/અજ્ઞાત સ્રોતોમાંથી એપ્લિકેશન ક્યારેય ડાઉનલોડ નહીં કરો
- ડાઉનલોડ લિંક પર અજાણતા ક્લિક કરવાનું ટાળીવે અજ્ઞાત સ્રોતોમાંથી પ્રાપ્ત એસએમએસ/ઈમેઈલ ડિલીટ કરો

#BankingDhyaanSe

ઓન કોલ/મોબાઈલ છેતરપિંડી વિશે (2)

મોડસ ઓપરેન્ડી

તમે સાવચેત અને સુરક્ષિત કઈ રીતે રહી શકો છો?

ઓટીપી આધારિત છેતરપિંડી

આ કઈ રીતે કરવામાં આવે છે

- તમને લોન અથવા ક્રેડિટ લિમિટમાં વધારાની ઓફર કરતી બેન્ક તરીકે ઠગો દ્વારા એસએમએસ પ્રાપ્ત થઈ શકે છે અને તમને મેસેજમાં ઉલ્લેખિત નંબર પર સંપર્ક કરવા પૂછવામાં આવી શકે છે
- તમે તે નંબર પર કોલ કરો ત્યારે તમને તમારી નાણાકીય વિગતો મોજૂદ હોય ત્યાં અમુક સ્વરૂપમાં (ઓનલાઈન પણ) ભરવા માટે પૂછવામાં આવે છે, જેને લીધે ઓટીપી અથવા પિનની વિગતો આપવા તમને સમજાવવાનું તેમને માટે આસાન બને છે, જેનાથી તમને નાણાકીય નુકસાન થાય છે

સુરક્ષાની ટિપ્સ

- તમારો ઓટીપી, પિન કે અંગત વિગતો કોઇને પણ કોઈ પણ સ્વરૂપમાં ક્યારેય આપશો નહીં
- તમારી જાણ બહાર ઓટીપી ઊપજાવવામાં નહીં આવે તેની ખાતરી રાખવા માટે નિયમિત રીતે તમારા એસએમએસ/ઈમેઈલ ચેક કરો

જ્યુસ જેકિંગ

આ કઈ રીતે કરવામાં આવે છે

- જ્યુસ જેકિંગ સાઈબર ચોરીનો પ્રકાર છે, જ્યાં તમારો મોબાઈલ કોઈ અજ્ઞાત/અનવેરિફાઈડ ચાર્જિંગ પોર્ટસ સાથે કનેક્ટ થવા પર અમુક અજ્ઞાત એપ્સ/માલવેર તમારા ડિવાઈસ પર ઈન્સ્ટોલ થઈ જાય છે, જેની સાથે ઠગો તમારો સંવેદનશીલ ડેટા, એસએમએસ કે સેવ કરેલો પાસવર્ડ ચોરી, કંટ્રોલ અને એક્સેસ કરી શકે છે

સુરક્ષાની ટિપ્સ

- જાહેર/અજ્ઞાત ચાર્જિંગ પોર્ટસ/કેબલ્સનો ઉપયોગ કરવાનું હંમેશાં ટાળો

ઓન કોલ/મોબાઈલ છેતરપિંડી વિશે (3)

મોડસ ઓપરેન્ડી

તમે સાવચેત અને સુરક્ષિત કઈ રીતે રહી શકો છો?

સિમ સ્વેપ છેતરપિંડી

આ કઈ રીતે કરવામાં આવે છે

- તમારા અકાઉન્ટની વિગતો અને ઓથેન્ટિકેશન તમારા રજિસ્ટર્ડ મોબાઈલ નંબર સાથે કનેક્ટેડ હોય છે. ઠગો તમારા નંબર માટે નવું રિપ્લેસમેન્ટ સિમ કાર્ડ પ્રાપ્ત કરીને નાણાકીય લેણદેણ કરવા માટે આવશ્યક ઓટીપી અને એલર્ટસને એક્સેસ મેળવવાનો પ્રયાસ કરે છે
- ઠગો તમારો ઓરિજિનલ સિમ બ્લોક કરવા અને તમારા મોબાઈલ નંબર સાથે નવું સિમ કલેક્ટ કરવા માટે તમારી સ્વાંગમાં તમારા મોબાઈલ ઓપરેટરના રિટેઈલ આઉટલેટમાં પહોંચી શકે છે
- વૈકલ્પિક રીતે તેઓ તમારા ઓપરેટર પાસેથી તેમને મોકલવામાં આવેલો એસએમએસ મોકલીને તમારું સિમ કાર્ડ અપગ્રેડ કરવા માટે તમને ડરાવી શકે અથવા આકર્ષિત કરી શકે છે, જેનાથી તમારું સિમ ડિએક્ટિવેટ થાય છે અને તેમના કબજામાંનું તમારા મોબાઈલ નંબર સાથેનું સિમ કાર્ડ એક્ટિવેટ થાય છે

સુરક્ષાની ટિપ્સ

- તમારો ગોપનીય અને અંગત ડેટા ચોરી કરવા માટે સોશિયલ એન્જિનિયરિંગ કૌભાંડથી સાવધાન રહો
- જો તમારો મોબાઈલ ફોન અચાનક કોઈ પણ નેટવર્ક કનેક્ટિવિટી નહીં બતાવે તો તમારા સિમ માટે કોઈ ડુપ્લિકેટ સિમ જારી તો નથી કરાયું ને તેની ખાતરી રાખવા માટે તમારી સેવાની સ્થિતિ વિશે તુરંત તમારા મોબાઈલ સેવા પ્રદાતા પાસે પૂછપરછ કરો

છેતરપિંડીના અન્ય પ્રકારો વિશે (1)

મોડસ ઓપરેન્ડી

તમે સાવચેત અને સુરક્ષિત કઈ રીતે રહી શકો છો?

સોશિયલ મિડિયા થકી ઠગાઈ

આ કઈ રીતે કરવામાં આવે છે

- ઠગો તમારો સ્વાંગ ધારણ કરે છે અને પ્રચલિત સોશિયલ મિડિયા મંચો પર નકલી અકાઉન્ટ તૈયાર કરે છે
- તમારો અનલોક ફોન અજાણતા હસ્તક અપાય (ઈમરજન્સી કોલ કરવા અથવા સમારકામ માટે) અથવા ફાજલ પડી રહ્યો હોય ત્યારે ઠગ તમારી પ્રોફાઈલ એક્સેસ કરવા તમારા મોબાઈલ નંબર પર મોકલવામાં આવેલો ઓટીપી પ્રાપ્ત કરી શકે છે અને અમુક એપ્લિકેશન્સના ડેસ્કટોપ વર્ઝન ઊપજાવી શકે છે, જેને લીધે તેમને તમારા સંપર્કો, ઓનલાઈન પ્રોફાઈલ અને ચેટ મેસેજીસને એક્સેસ મળે છે
- તેઓ તુરંત તબીબી મદદ વગેરે માટે નાણાં પૂછીને તમારા મિત્રોને વિનંતી મોકલી શકે છે

સુરક્ષાની ટિપ્સ

- કોઈ પણ પેમેન્ટ કરવા પૂર્વે ફોન અથવા વ્યક્તિગત રીતે તમારા સંપર્કો સુધી પહોંચીને વિનંતીની ઓથેન્ટિસિટી વેરિફાઈ કરો
- તમારો ફોન લોક કર્યા વિના ક્યારેય ફાજલ છોડશો નહીં

ક્યુઆર સ્કેન– આધારિત છેતરપિંડી

આ કઈ રીતે કરવામાં આવે છે

- ઠગો વિવિધ બહાનાં હેઠળ તમારો સંપર્ક કરી શકે છે અને પેમેન્ટ એપ્સનો ઉપયોગ કરીને અને પેમેન્ટ પ્રોસેસ પૂર્ણ કરીને ક્યુઆર કોડ્સ સ્કેન કરવા તમને લલચાવી શકે છે
- આ ક્યુઆર કોડ્સમાં પૂર્વવ્યાખ્યા કરેલી અકાઉન્ટની વિગતો હોય છે, જેનાથી કોઈ ચોક્કસ અકાઉન્ટમાં રકમ ટ્રાન્સફર કરવામાં આવે છે, જે ઠગો દ્વારા તમારા અકાઉન્ટમાંથી નાણાં ટ્રાન્સફર પૂર્ણ કરવા માટે યુક્તિ કરીને ચેડાં કરી શકે છે

સુરક્ષાની ટિપ્સ

- પેમેન્ટ એપ્સનો ઉપયોગ કરીને કોઈ પણ ક્યુઆર કોડ્સ સ્કેન કરવા સમયે સાવચેત રહો

#BankingDhyaanSe

છેતરપિંડીના અન્ય પ્રકારો વિશે (2)

મોડસ ઓપરેન્ડી

તમે સાવચેત અને સુરક્ષિત કઈ રીતે રહી શકો છો?

લોટરી અથવા નોકરીમાં છેતરપિંડીનું કૌભાંડ

આ કઈ રીતે કરવામાં આવે છે

- ઠગો તમે મોટી લોટરી/ઈનામ જીત્યું છે એવી માહિતી આપીને અથવા નોકરી ઓફર કરતી નામાંકિત કંપનીના અધિકારીના સ્વાંગમાં ઈમેઈલ મોકલે અથવા ફોન કોલ્સ કરે છે
- જોકે નાણાં/ભેટ પ્રાપ્ત કરવા અથવા પસંદગી પ્રક્રિયા પૂરી કરવા માટે તમને ઉપલક અમુક નાણાં ચૂકવવા માટે પૂછી શકે છે
- વિનંતી કરેલી રકમ સામાન્ય રીતે લોટરી/ઈનામ કરતાં બહુ નાની ટકાવારી હોવાથી અથવા નોકરી મેળવવા માટે મહત્ત્વપૂર્ણ હોવાનું ધ્યાનમાં રાખીને તમે આવા પેમેન્ટ કરવા મજબૂર બની શકો છો

સુરક્ષાની ટિપ્સ

- કોઈ પણ લોટરીના કોલ્સ/ઈમેઈલ્સ સામે પેમેન્ટ નહીં કરી અથવા તમારી સંરક્ષિત ક્રિડેન્શિયલ્સ શેર નહીં કરો
- કોઈ પણ માની નહીં શકાય તેવી લોટરી કે ઓફરોની વિશ્વસનીયતા સામે હંમેશાં પ્રશ્ન કરો
- યાદ રાખો, કોઈ પણ અસલી કંપની નોકરી માટે ક્યારેય નાણાં માગતી નથી

એટીએમ કાર્ડ સ્કિમિંગ

આ કઈ રીતે કરવામાં આવે છે

- ઠગો દ્વારા ડેટા ચોરી કરવા, ડુપ્લિકેટ કાર્ડ બનાવવા અને તમારા અકાઉન્ટમાંથી નાણાં ઉપાડવા માટે એટીએમ મશીન્સમાં સ્કિમિંગ ડિવાઈસીસ ઈન્સ્ટોલ કરે છે.
- તેઓ તમારા દ્વારા એન્ટર કરેલી માહિતી કેપ્ચર કરવા માટે ડમી કીપેડ્સ અથવા ઝીણો કેમેરા ઈન્સ્ટોલ પણ કરી શકે છે
- તેઓ તમે એન્ટર કરો ત્યારે તમારો પિન જોવા એટીએમ સેવાનો ઉપયોગ કરવા આવેલા ગ્રાહક તરીકે પણ સ્વાંગ રચી શકે છે અથવા તમે રોકડ ઉપાડી નહીં શકો તો તમારી લેણદેણ પૂરી કરવા તમને મદદરૂપ થવાની ઓફર કરી શકે છે

સુરક્ષાની ટિપ્સ

- સતર્ક રહો અને એટીએમ મશીનના કાર્ડ ઈન્સર્શન સ્લોટ અથવા કીપેડ નજીક કોઈ વધારાનું ડિવાઈસ જોડાયેલું નથી ને તેની ખાતરી રાખો
- નજીકમાં કોઈ પણ ઊભું હોય તેની હાજરીમાં કાર્ડની વિગતો એન્ટર નહીં કરો
- પિન એન્ટર કરતી વખતે કીપેડ કવર કરો અને તમારું કાર્ડ કે પિન કોઇને પણ આપશો નહીં
- જો કશું પણ શંકાસ્પદ જણાય તો તુરંત એટીએમ સંકુલની બહાર નીકળી જાઓ

#BankingDhyaanSe

શંકાસ્પદ અથવા છેતરપિંડીની લેણદેણ એક્સિસ બેન્કને જાણ કરો

જો તમને શંકાસ્પદ લેણદેણ જણાય અથવા છેતરપિંડીની લેણદેણ થયાનું જણાય તો તમે નીચે ઉલ્લેખિત ચેનલો સુધી પહોંચી શકો છોઃ

- અમારા ફોન બેન્કિંગ નંબરો પર કોલ કરોઃ 1860 419 5555/1860 500 5555
- અમને લખોઃ https://www.axisbank.com/support/
- કોઈ પણ એક્સિસ બેન્ક શાખામાં પહોંચી જાઓ

તમારો સમય અને તમે ધ્યાન આપ્યું તે માટે તમારો આભાર.

#BankingDhyaanSe