સ્કેમર્સ અહીં,

સ્કેમર્સ ત્યાં,

ક્યાંય ફસાઈ જશો નહીં!

#BankingDhyaanSe 2.0

AXIS BANK

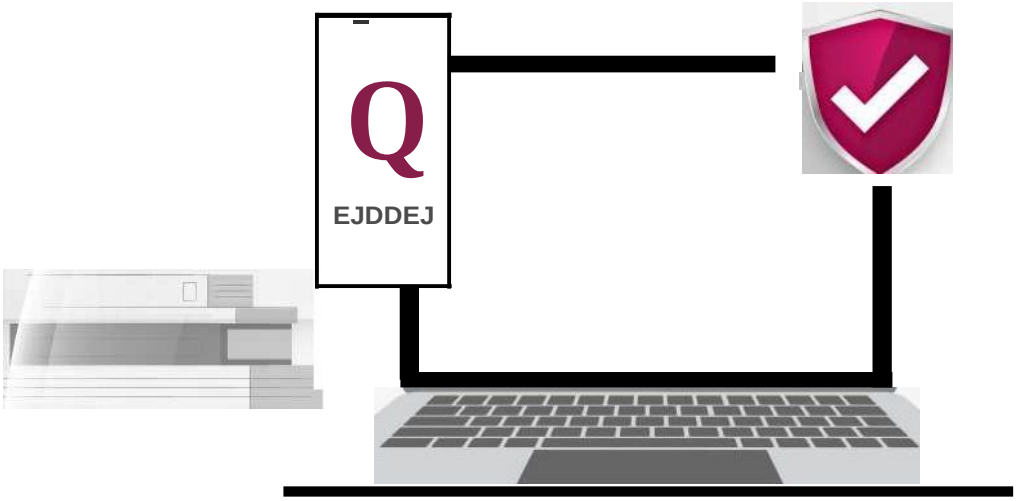
તમે કમાવવા માટે સખત મહેનત કરો છો,
શા માટે તમારી કમાણી સુરક્ષિત ન રાખો?

એક્સિસ બેંક ફ્રોડ અવેરનેસ બુકલેટ **#BankingDhyaanSe 2.0** માં આપનું સ્વાગત છે,

નાણાકીય કૌભાંડોને સમજવા અને અટકાવવા માટેની આ તમારી ચાવી. ઝડપથી વિકસતા ડિજિટલ યુગમાં, જ્ઞાન એ છેતરપિંડી કરનારાઓ સામે તમારું કવચ છે. આ માર્ગદર્શિકા તમને તમારા મહેનતથી કમાયેલા નાણાંને સુરક્ષિત રાખવા માટે આંતરદૃષ્ટિ, વાસ્તવિક જીવનના ઉદાહરણો અને વ્યવહારુ ટિપ્સ પ્રદાન કરે છે.

બેંકિંગમાં તમારા વિશ્વાસુ ભાગીદાર તરીકે, Axis Bank(એક્સિસ બેંક) તમને વિશ્વાસપૂર્વક ડિજિટલ લેન્ડસ્કેપમાં નેવિગેટ(શોધખોળ) કરવામાં મદદ કરવા માટે સમર્પિત છે. ચાલો છેતરપિંડી સામે રક્ષણ કરીએ અને સાથે મળીને ઉજ્જવળ નાણાકીય ભવિષ્ય સુરક્ષિત કરીએ.

OTP કૌભાંડો



વન-ટાઇમ પાસવર્ડ એ તમારા અભેદ્ય ડિજિટલ સામ્રાજ્યને ઍક્સેસ કરવા માટે એક સુવર્ણ ચાવી છે.

તમારી કીમતી ચાવી ચોરતા ધૂર્ત યુક્તિઓને દૂર રાખવા માટે, તમારે તમારા કિલ્લાના રક્ષક બનવું પડશે!

OTP ને ગોપનીય રાખો: ફોન કોલ્સ, ઈ-મેઈલ, ટેક્સ્ટ મેસેજ અથવા સોશિયલ મીડિયા દ્વારા OTP ક્યારેય કોઈની સાથે શેર કરશો નહીં અને સાવધાન રક્ષકની જેમ સાવચેત રહો.

વિનંતીઓ ચકાસો: વિશ્વાસ કરો પણ ચકાસો. જો કોઈ OTP વિનંતી વાદળી રંગની બહાર આવે છે અથવા શંકાસ્પદ લાગે છે, તો ઉતાવળ કરશો નહીં. તમે પ્રતિક્રિયા આપો તે પહેલાં તેની અધિકૃતતા બે વાર તપાસો.

અધિકૃત વેબસાઇટ્સ અથવા એપ્સનો ઉપયોગ કરો: OTP શેર કરતી વખતે સુરક્ષિત રહો. હંમેશા સત્તાવાર સાઇટ અથવા એપ્લિકેશનની સીધી મુલાકાત લો - કોઈ શૉર્ટકટ નહીં. ટાઈપ કરવાથી કોઈપણ દિવસે લિંક પર ક્લિક થાય છે.

તાકીદની વિનંતીઓથી સાવધ રહો: સ્કેમર્સ વારંવાર તમારો OTP શેર કરવા માટે તમારા પર દબાણ લાવવા માટે તાકીદની ભાવના પેદા કરે છે. એક પગલું પાછળ લો, વિવેચનાત્મક રીતે વિચારો અને કાર્ય કરતા પહેલા વિનંતીને સ્વતંત્ર રીતે ચકાસો.

દ્વિ-પરિબળ પ્રમાણીકરણ સક્ષમ કરો: 2FA (ટુ-ફેક્ટર ઓથેન્ટિકેશન) સાથે સુરક્ષા પર બમણી ઘટાડો. ઍપ-આધારિત અથવા હાર્ડવેર ટોકન્સ જેવા રોક-સોલિડ(સખત) વિકલ્પો પસંદ કરો. તેઓ કોઈપણ દિવસે SMS OTP કરતાં વધી જાય છે.

મહેરબાની કરીને યાદ રાખો, બેંક તમારા CVV, OTP, PIN, કાર્ડ નંબર, પાસવર્ડ વગેરે માટે પૂછશે નહીં. આ વિગતો કોઈની સાથે શેર કરશો નહીં.

ક્રેડિટ કાર્ડ કૌભાંડો

ચાલો ક્રેડિટ કાર્ડ સ્કેમ્સને છુપાવવા અને શોધવાની એક સ્નીકી ગેમ તરીકે કલ્પના કરીએ. જેમ કે કોઈ સ્કેમર તેમના સાચા ઈરાદાઓને છુપાવવાનો પ્રયાસ કરે છે, તેમ તેઓ તમને તમારી ક્રેડિટ કાર્ડ માહિતી જાહેર કરવા માટે છેતરશે.

તેમની જાળમાં ન આવવા માટે, આ ટીપ્સને ધ્યાનમાં રાખો:

ફિશર્સથી સાવચેત રહો: સ્કેમર્સ તમારી બેંક અથવા પરિચિત કંપનીના હોવાનો ડોળ કરી શકે છે. તેમની યુક્તિઓ માટે પડશો નહીં; તેમની ઓળખ ચકાસો.

1i તમારા સ્ટેટમેન્ટ તપાસો: તમારા ક્રેડિટ કાર્ડ સ્ટેટમેન્ટની નિયમિત સમીક્ષા કરો. જો તમે અજાણ્યા ખર્ચ અથવા શુલ્ક દેખાય, તો તે રમતમાં છુપાયેલા ખેલાડીઓને શોધવા જેવું છે-તેમને તરત જ સંબોધિત કરો.

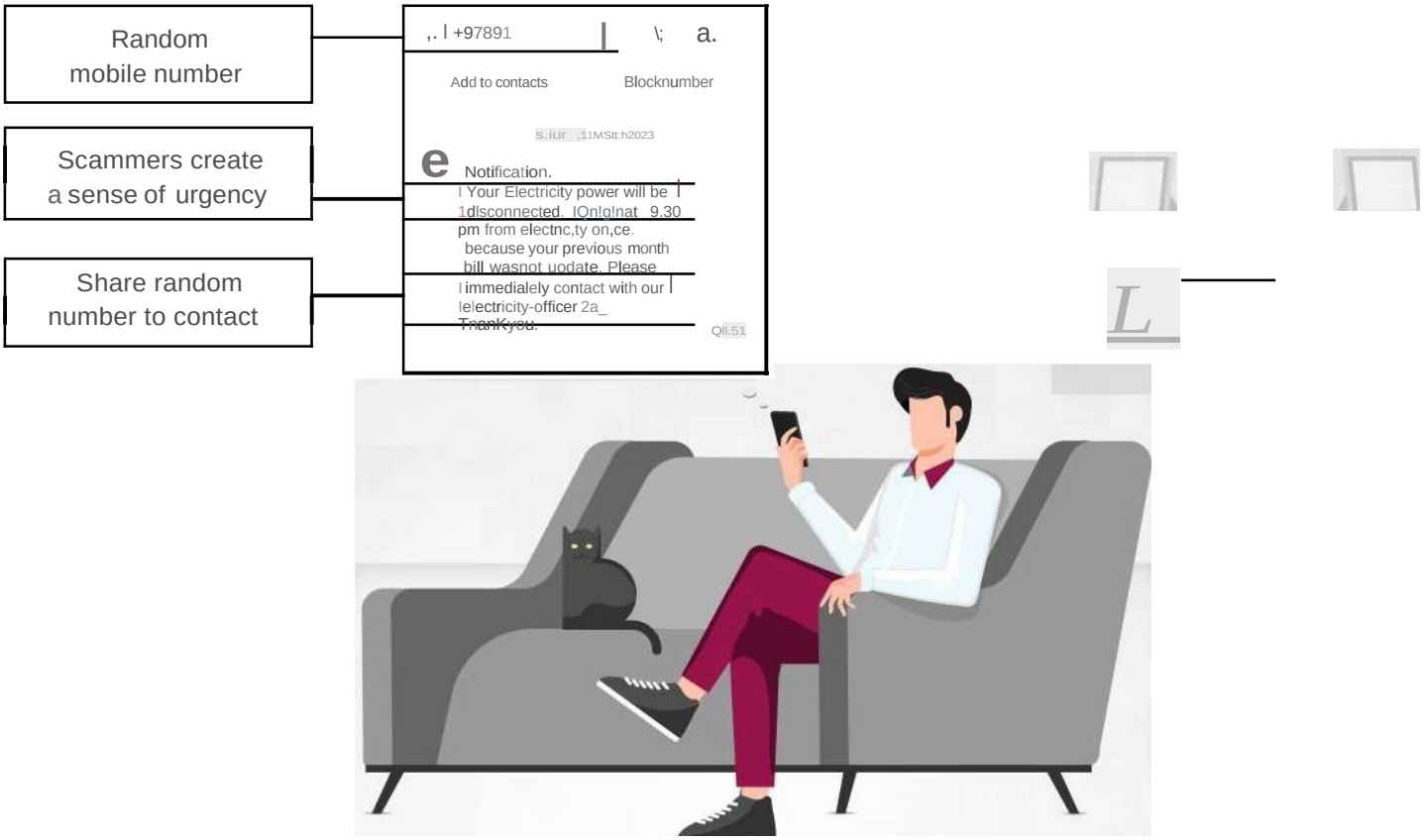
ટ્રાન્ઝેક્શન મર્યાદા સેટ કરો: તમારી બધી પેમેન્ટ ચેનલ્સ પર ટ્રાન્ઝેક્શન લિમિટ સેટ કરો અને તમારી જરૂરિયાત મુજબ 'મેનેજ યુસેજ' સેક્શનને કસ્ટમાઇઝ કરો.

ફક્ત સુરક્ષિત સાઇટ્સ: ઓનલાઈન ખરીદી કરતી વખતે, ખાતરી કરો કે વેબસાઇટ સુરક્ષિત છે (URL માં "https" જુઓ). તે રમત માટે સલામત રમતનું મેદાન પસંદ કરવા જેવું છે.

અપડેટ રહો: જેમ તમે રમતમાં નવી વ્યૂહરચના શીખો છો તેમ, કૌભાંડની નવીનતમ યુક્તિઓ પર નજર રાખો. આ રીતે, તમે સ્કેમર્સને આઉટસ્માર્ટ કરવા માટે તૈયાર થશો.

વીજળી બિલની છેતરપિંડી

નકલી SMS કેવી રીતે ઓળખવો?



આને ચિત્રિત કરો: જ્યારે તમે ઘરે આરામની સાંજનો આનંદ માણી રહ્યાં છો, તમારો મનપસંદ શો જોઈ રહ્યાં છો. ત્યારે તમારો ફોન ઇનકમિંગ મેસેજ સાથે બઝ કરે છે, તે તમારો વીજળી પ્રદાતા છે અને તેઓ દાવો કરી રહ્યાં છે કે તમારા તાજેતરના બિલ માટે તમારી પાસે વધુ પડતી રકમ બાકી છે.

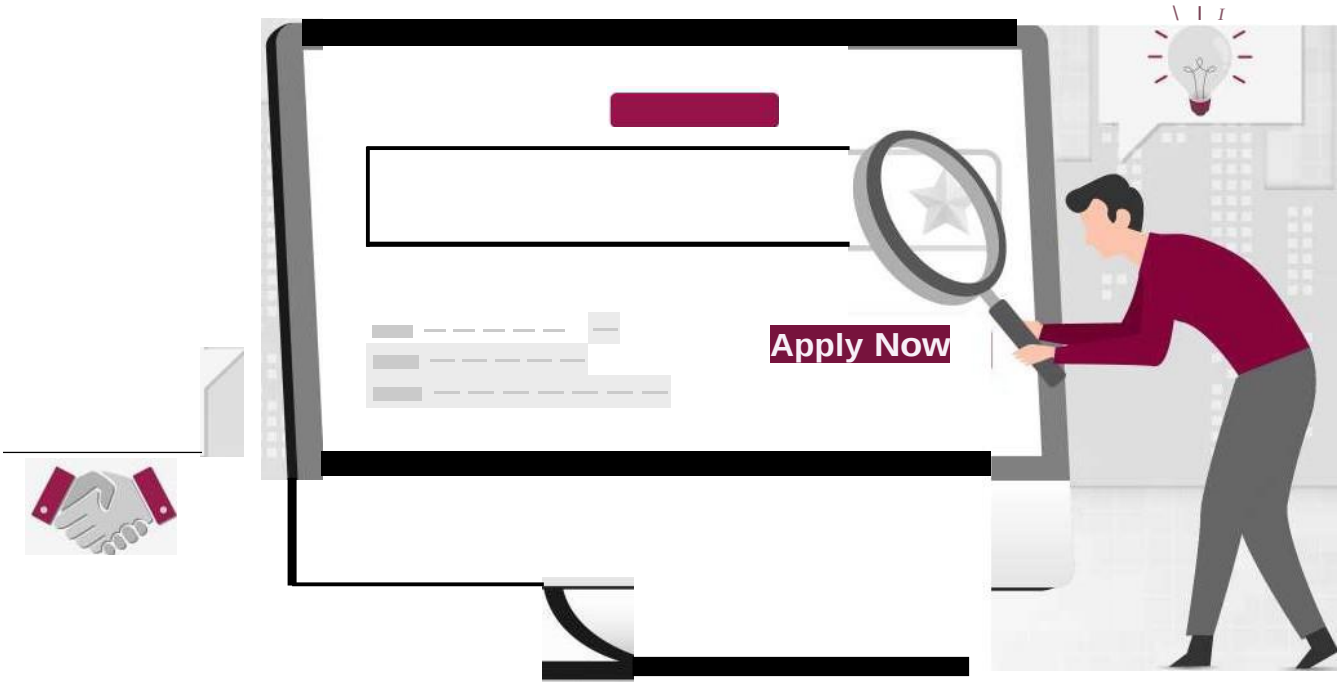
તમે ગભરાઓ તે પહેલાં, આનો વિચાર કરો: વીજળીના બિલની છેતરપિંડી, એક છૂપી ભૂતની જેમ, ચેતવણી વિના તમારા જીવનમાં ઘૂસી શકે છે.

તમારી ગોપનીય વિગતો ક્યારેય કોઈની સાથે શેર કરશો નહીં અથવા અણગમતી લિંક પર ક્લિક કરશો નહી.

બિલની ચુકવણી કરવા માટે માત્ર અધિકૃત અને સુરક્ષિત વેબસાઇટનો ઉપયોગ કરો.

યાદ રાખો, વીજળી વિભાગ ક્યારેય વ્યક્તિગત વિગતો અથવા રેન્ડમ/અનનોંધાયેલ નંબરો દ્વારા ચૂકવણી માટે પૂછતો નથી.

નોકરી કૌભાંડો



કલ્પના કરો કે તમે જોબ લિસ્ટિંગમાં સ્ક્રોલ કરી રહ્યાં છો, અને અચાનક તમે એવી નોકરીની ઑફર પર ઠોકર ખાઓ છો જે સાચી નથી લાગતી. અમર્યાદિત વેકેશનના દિવસો, તમારા પાયજામામાં કામ અને ડેટા એન્ટ્રી માટે છ આંકડાનો પગાર? મને સાઇન અપ કરો!

રાહ જુઓ, તમે તે "હવે લાગુ કરો" બટનને હિટ કરો તે પહેલાં!

કંપનીનું સંશોધન કરો: કંપનીને ઑનલાઇન જુઓ અને ખાતરી કરો કે તે પ્રતિષ્ઠિત છે. સ્કેમર્સ ઘણીવાર ખાતરી આપતી વેબસાઇટ્સ સાથે નકલી કંપનીઓ બનાવે છે.

અગાઉથી ચૂકવણી કરશો નહીં: તમે કામ કરવાનું શરૂ કરો તે પહેલાં કાયદેસર નોકરીદાતાઓ તમને તાલીમ, સામગ્રી અથવા પૃષ્ઠભૂમિ તપાસ માટે ચૂકવણી કરવાનું કહેશે નહીં.

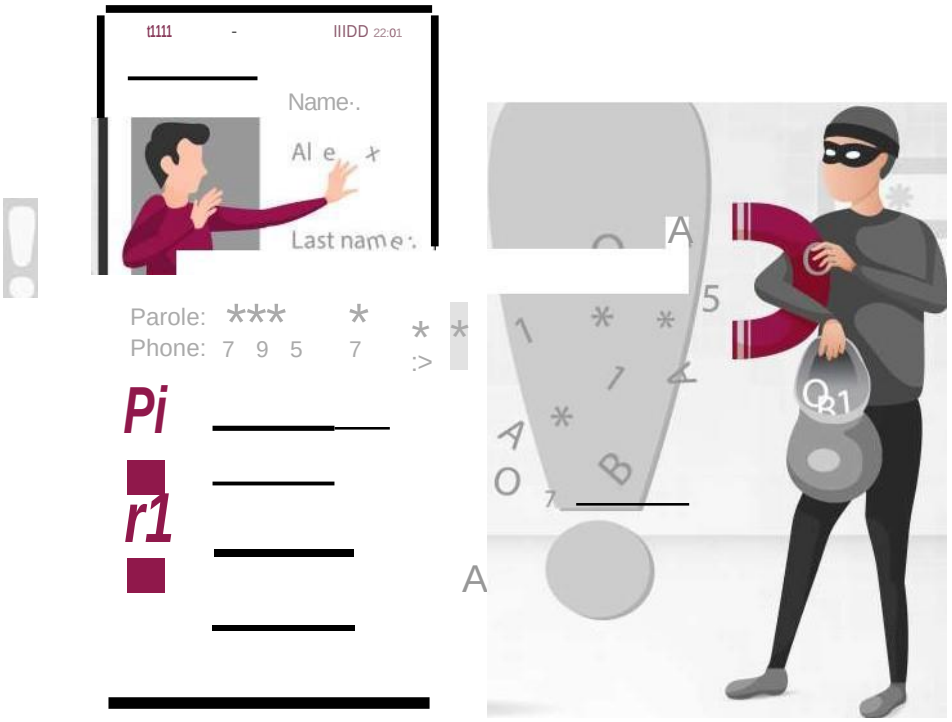
લાલ ધ્વજ માટે જુઓ: જો નોકરી માટે તમારે તમારા સામાજિક સુરક્ષા નંબર અથવા નાણાકીય વિગતો જેવી સંવેદનશીલ માહિતી તરત જ પ્રદાન કરવાની જરૂર હોય તો સાવચેત રહો.

ભાડે આપવા માટે ખૂબ જ ઝડપી: જો તમને ઇન્ટરવ્યુ વિના અથવા વધુ માહિતીની આપલે કર્યા વિના સ્થળ પર જ નોકરીની ઓફર કરવામાં આવે, તો તે કૌભાંડ હોઈ શકે છે.

તમારી વૃત્તિ પર વિશ્વાસ કરો: જો કંઈક ખરાબ લાગે છે, તો તમારા ગટ્સ(દૃઢનિશ્ચય) પર વિશ્વાસ કરો અને સાવધાની સાથે આગળ વધો અથવા દૂર જાઓ.

યાદ રાખો, જ્યારે નોકરીની શોધ તમારી પ્રથમ પ્રાથમિકતા હોવી જોઈએ ત્યારે તમારી વ્યક્તિગત અને નાણાકીય માહિતીની સુરક્ષા કરવી.

કૉલ સ્પૂફિંગ કૌભાંડો



જેમ કે કોઈ જાદુગર વસ્તુઓને તેઓ જે છે તેનાથી અલગ દેખાડે છે તેમ, સ્કેમર્સ તમારા કૉલર આઈડીની હેરફેર કરી શકે છે જેથી એવું લાગે કે તેઓ કોઈ તમને જાણતા હોય અથવા વિશ્વાસ કરે છે - આ કિસ્સામાં, તમારી બેંક તેમની સાચી ઓળખ માટે એક ડિજિટલ વેશ સમાન છે.

આ સ્નીકીચતુર) યુક્તિથી પોતાને બચાવવા માટે, આ ટીપ્સ યાદ રાખો:

સાવધાની સાથે ચકાસો: જો કોલર ID પરિચિત લાગે તો પણ શંકાશીલ રહો. જો કોઈ વ્યક્તિ સંવેદનશીલ માહિતી માટે પૂછે છે, તો અન્ય માધ્યમો દ્વારા તેમની ઓળખને બે વાર તપાસો.

વ્યક્તિગત માહિતી શેર કરશો નહીં: ફોન પર ક્યારેય વ્યક્તિગત અથવા નાણાકીય માહિતી આપશો નહીં, ભલે કૉલર કાયદેસર લાગે. વિશ્વાસપાત્ર નંબરનો ઉપયોગ કરીને હેંગ અપ કરો અને પાછા કૉલ કરો.

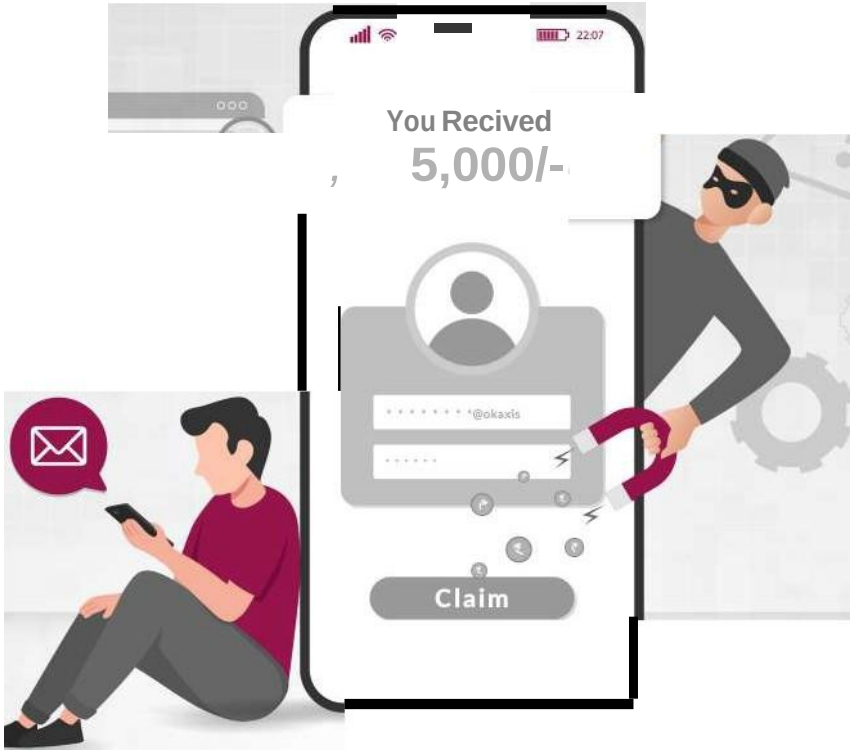
ખાનગી રહો: તમે ઑનલાઇન અથવા સોશિયલ મીડિયા પર કઈ અંગત વિગતો શેર કરો છો તો તેના વિશે સાવચેત રહો. સ્કેમર્સ વારંવાર તેમના સ્પુફ કરેલા કૉલ્સને વધુ વિશ્વાસપાત્ર બનાવવા માટે આ સ્ત્રોતોમાંથી માહિતી એકત્ર કરે છે.

કૉલ બ્લૉકિંગનો ઉપયોગ કરો: કૉલ-બ્લોકિંગ ઍપ અથવા તમારા ફોન કૅરિઅર દ્વારા પ્રદાન કરવામાં આવેલી સુવિધાઓનું અન્વેષણ કરો. તેઓ સંભવિત સ્કેમ કૉલ્સને ફિલ્ટર કરવામાં મદદ કરી શકે છે.

Google અથવા કોઈપણ સર્ચ એન્જિન પર ફોન નંબરો શોધશો નહીં. જો તમે આમ કરો છો, તો એન્ટિટી અથવા વેપારી દ્વારા તમને મોકલવામાં આવેલી કોઈપણ લિંક પર ક્લિક કરશો નહીં.

વધુમાં, કૃપા કરીને ખાતરી કરો કે તમારી પાસે ફક્ત અધિકૃત એપ્લીકેશન સ્ટોર્સ પરથી તમારા ઉપકરણો પર ડાઉનલોડ થયેલ બેંકિંગ એપ્લિકેશનના નવીનતમ સંસ્કરણો છે.
કૃપા કરીને સમયાંતરે આ તપાસતા રહો. યાદ રાખો, જેમ તમે વાસ્તવિક જીવનમાં માસ્ક પહેરેલા અજાણ્યા વ્યક્તિ પર વિશ્વાસ કરશો નહીં, તેમ ફોન પર માસ્ક પહેરેલા કૉલર પર વિશ્વાસ કરશો નહીં. જાગ્રત રહો!

UPI રિફંડ કૌભાંડો



કલ્પના કરો કે જ્યારે તમે UPI રિફંડ નોટિફિકેશન જોશો ત્યારે તમે તમારા ફોનમાં સ્ક્રોલ કરી રહ્યાં છો અને અચાનક તમે ક્લાઉડ નવ પર છો! પણ રાહ જુઓ. આ UPI રિફંડ કૌભાંડ હોઈ શકે છે!

UPI અથવા ધ યુનિફાઇડ પેમેન્ટ્સ ઇન્ટરફેસ આપણા રોજિંદા જીવનનો એક ભાગ બની ગયો છે. તમારા સ્થાનિક કિરાણા સ્ટોર્સ પર ચૂકવણી કરવાથી લઈને ફોન રિચાર્જ કરવા માટે, ફ્લાઇટ ટિકિટ બુક કરવા સુધી, આપણે વિવિધ વસ્તુઓ માટે UPI ચુકવણીનો ઉપયોગ કરીએ છીએ. તેથી છેતરપિંડી કરનારાઓએ UPI એપ્સનો ઉપયોગ કરીને લોકોને ફસાવવા માટે નવી રીતો અપનાવવાનું શરૂ કર્યું છે.

તેમની સત્તાવાર ભાષા અને વ્યાવસાયિક ભાષા માં ક્યારેય પડવું નહીં. નીચેની ટીપ્સ ધ્યાનમાં રાખો:

લિંક્સથી સાવચેત રહો: સ્કેમર્સ તમને એક લિંક મોકલી શકે છે, જે તમને રિફંડનો દાવો કરવા માટે નોંધણી કરવા વિનંતી કરે છે.

ઉચ્ચ-દબાણની યુક્તિઓ: તેઓ તમને તાત્કાલિક નાણાં માટે તરત જ બેંક વિગતો અથવા UPI પિન ભરવા માટે દબાણ કરશે.

યોગ્યતા ચકાસો: ખાતરી કરો કે તમે રિફંડ માટે પાત્ર છો. જો હા, તો વિશ્વસનીય સ્ત્રોત માટે તપાસો.

યાદ રાખો, બેંક અથવા અન્ય અધિકારીઓ તમને આવી સંવેદનશીલ વિગતો માટે ક્યારેય પૂછશે નહીં.

ફિશિંગ કૌભાંડો

કલ્પના કરો કે તમે તમારા પોતાના વ્યવસાયને ધ્યાનમાં રાખીને સ્વચ્છ તળાવમાં શાંતિથી સ્વિમિંગ કરતી માછલી છો. અચાનક, એક ચળકતી, આકર્ષક લાલચ તમારી સામે લટકશે. તમે રસપ્રદ છો, પરંતુ રાહ જુઓ - કંઈક ગૂંચવણભર્યું છે!

ફિશિંગ સ્કેમ્સ સાથે ડિજિટલ ક્ષેત્રમાં આવું જ થાય છે.

સાયબર અપરાધીઓ તમને સંવેદનશીલ માહિતી જાહેર કરવા માટે ભરોસાપાત્ર વ્યક્તિઓ તરીકે રજૂ કરે છે, જેમ કે માછલી લાલચ દ્વારા લલચાય છે. તેઓ નકલી ઇમેઇલ્સ, સંદેશાઓ અથવા વેબસાઇટ્સ મોકલે છે જે કાયદેસર લાગે છે, ઘણીવાર બેંકો, સોશિયલ મીડિયા અથવા તમારા બોસનું અનુકરણ પણ કરે છે.

આ ડિજિટલ હુક્સને ડોજ(છળકપટ) કરવા માટે, આ ટીપ્સ યાદ રાખો:

URL ને બે વાર તપાસો: તેઓ ખરેખર ક્યાં દોરી જાય છે તે જોવા માટે લિંક્સ પર હોવર કરો.

વ્યક્તિગત માહિતી શેર કરશો નહીં: કાયદેસર સંસ્થાઓ ઈમેલ દ્વારા સંવેદનશીલ સામગ્રી માટે પૂછશે નહીં.

rl2J

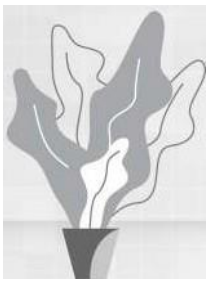
શંકાસ્પદ રહો: અણધારી વિનંતીઓ? કાર્ય કરતા પહેલા અન્ય માધ્યમો દ્વારા ચકાસો.

l@l:'"\,.

સુરક્ષા સૉફ્ટવેર અપડેટ કરો: તમારા ડિજિટલ તળાવને નવીનતમ સંરક્ષણો સાથે સુરક્ષિત રાખો.

સાવધ માછલીની જેમ સાવધ રહો અને ઈન્ટરનેટના વિશાળ મહાસાગરમાં ચતુરાઈથી તરી જાઓ!

વિશીંગ કૌભાંડો



a

તમારા ફોનની રિંગ વાગે છે, અને તે તમારી કહેવાતી બેંક છે અને તમારા ખાતામાં કોમ્પ્રોમાઇઝ(સમાધાન) થયા હોવાનો દાવો કરતી 'તાત્કાલિક' કૉલ સાથે, અથવા કદાચ 'વિજેતા' કૉલ એવો દાવો કરે છે કે તે તમારો ભાગ્યશાળી દિવસ છે, અને તમે આશ્ચર્યજનક કંઈક જીતી ગયા છો!

ફોન પકડી રાખો (શાબ્દિક)!

આવા કૌભાંડોથી સુરક્ષિત રહેવા માટે, નીચેની ટીપ્સ યાદ રાખો:

ફોન પર તમારી અંગત વિગતો ક્યારેય ન ફેલાવો.

<@)> શેરલોક હોમ્સ બનો જાઓ અને તે કોલરની ઓળખ ચકાસી કાઢો.

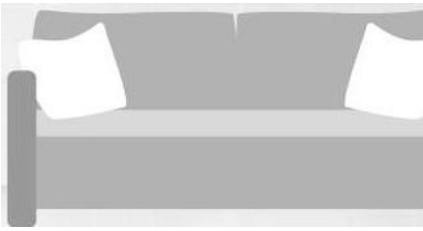
નાટક માં પડશો નહીં! જ્યારે તેઓ ગરમીથી ચાલુ કરે ત્યારે તમે ઠંડા રહો.

ઓનલાઈન અજાણ્યાઓ સાથે માહિતી શેર કરવામાં સાવચેત રહેવાનું યાદ રાખો - તમારી સામગ્રી(માહિતી)ને સુરક્ષિત રાખવા માટે સ્માર્ટ રહો!

UPI કૌભાંડો – નાણા વિકલ્પની વિનંતી કરો.

, +75,000/-

, -75,000/-



સ્નેહાએ ઓનલાઈન ખરીદી અને વેચાણ એપ પર તેના ફર્નિચરની જાહેરાત કરી. અર્ધલશ્કરી દળના જવાનો હોવાનો દાવો કરતા ખરીદદારે વોટ્સએપ પર ચુકવણી માટે QR કોડ મોકલ્યો હતો. સ્નેહાએ તેને સ્કેન કર્યું અને 75,000 ગુમાવ્યા.

શું આ પરિચિત લાગે છે? શું તમે UPI પેમેન્ટ પ્લેટફોર્મના વારંવાર ઉપયોગને કારણે UPI છેતરપિંડીનો શિકાર થવાનો ડર અનુભવો છો?

હંમેશા યાદ રાખો:

UPI પિન ફક્ત ચુકવણી કરવા માટે જરૂરી છે અને કોઈપણ ચુકવણી પ્રાપ્ત કરવા માટે નહીં.

તમારો OTP, UPI PIN અથવા કોઈપણ ગોપનીય વિગતો કોઈની સાથે શેર કરશો નહીં.

તમારા UPI પિનને ચુકવણી મેળવવા માટે કહેવામાં આવે તે ક્ષણે પોતાને રોકો! આ વાસ્તવમાં ચુકવણીની વિનંતી હોઈ શકે છે અને એકત્રિત વિનંતી નથી.

કોઈપણ ચુકવણી શરૂ કરતા પહેલા હંમેશા UPI એપ્લિકેશનમાં મોબાઈલ નંબર અને નામની ચકાસણી કરો.

QR કોડ સ્કેન છેતરપિંડી

પેમેન્ટ એપ પર સાવધાની સાથે QR કોડ સ્કેન કરો;
તેઓ મની ટ્રાન્સફર માટે એકાઉન્ટ વિગતો ધરાવે છે.

પૈસા મેળવવા માટે QR કોડ સ્કેન કરશો નહીં; ભંડોળ મેળવવા માટેના વ્યવહારોમાં બારકોડ/QR કોડ સ્કેન કરવું અથવા મોબાઇલ બેંકિંગ PIN (m-PIN), પાસવર્ડ વગેરે દાખલ કરવું બિનજરૂરી છે.

ગેરવ્યાજબી ઉતાવળ અથવા તાકીદ બતાવનાર ખરીદનાર/વિક્રેતા મોટે ભાગે છેતરપિંડી કરનાર હોય છે. શાંત રહો, હંમેશા સ્પષ્ટતા શોધો અને જરૂરી પ્રશ્નો પૂછો.

વણચકાસેલ મોબાઈલ એપ છેતરપિંડી

તમને લાંબા સમયથી ખોવાયેલા પિતરાઈ ભાઈ તરફથી એક SMS, ઈમેઈલ અથવા તો એક સંદેશ પ્રાપ્ત થાય છે જે તમે ક્યારેય અસ્તિત્વમાં નથી જાણતા, આ બધું તમારી મનપસંદ અધિકૃત એન્ટિટીની કાયદેસર એપ્લિકેશનની જેમ દેખાતી લિંક સાથે.

એક મિનિટ રાહ જુઓ! આ મૈત્રીપૂર્ણ ડાઉનલોડ્સ નથી; તે ડિજિટલ પાર્ટીના આમંત્રણો છે જેમાં તમે ચોક્કસપણે અટેન્ડ કરવા(હાજરી આપવા) માંગતા નથી!

સ્કેમર્સ SMS ઇમેઇલ અથવા સોશિયલ મીડિયા દ્વારા નકલી એપ્લિકેશન લિંક્સ મોકલે છે જે કાયદેસર જેવી લાગે છે. તેઓ વપરાશકર્તાઓને તેમના પર ક્લિક કરવા માટે સમજાવે છે, જેનાથી અજાણી એપ્સ ડાઉનલોડ થાય છે. એકવાર ઇન્સ્ટોલ થઈ ગયા પછી, સ્કેમર્સ ગોપનીય માહિતી અને OTP સહિત ઉપકરણની ઍક્સેસ મેળવે છે.

અજાણ્યા સ્ત્રોતોમાંથી અથવા અજાણ્યા લોકોની વિનંતી પર એપ્સ ડાઉનલોડ કરવાનું ટાળો.

ડાઉનલોડ કરતા પહેલા એપ્લિકેશન પ્રકાશકો અને વપરાશકર્તા રેટિંગ્સ ચકાસો.

પરવાનગીઓ અને એપ્લિકેશન વિનંતીઓ (દા.ત. સંપર્કો, ફોટા) ની સમીક્ષા કરો અને ફક્ત જરૂરી હોય તે જ આપો.

યાદ રાખો, બેંક અથવા અન્ય અધિકારીઓ તમને આવી સંવેદનશીલ વિગતો માટે ક્યારેય પૂછશે નહીં.

ATM કાર્ડ સ્કિમિંગ છેતરપિંડી

ડિજિટલ પિકપોકેટિંગ જેવા ATM સ્કિમિંગ વિશે વિચારો. જ્યારે તમે પૈસા ઉપાડવા અથવા તમારું બેલેન્સ તપાસવા માટે ATM નો ઉપયોગ કરો છો, ત્યારે છેતરપિંડી કરનારાઓ તમારી કાર્ડની માહિતી રેકોર્ડ કરવા માટે મશીન પર છુપાયેલા ઉપકરણો સેટ કરે છે. આ ઉપકરણો નકલી કાર્ડ સ્લોટ અથવા નાના કેમેરા જેવા અસ્પષ્ટ હોઈ શકે છે.

ATMની તપાસ કરો: ATMનો ઉપયોગ કરતા પહેલા કોઈપણ અસામાન્ય જોડાણો, છૂટા ભાગો અથવા છુપાયેલા કેમેરા માટે હંમેશા કાર્ડ સ્લોટ અને કીપેડ તપાસો.

તમારો **PIN** કવર કરો: તમારી PIN એન્ટ્રીને તમારા હાથ અથવા શરીર વડે ઢાંકી દો, જેથી કેમેરા અથવા દર્શકો માટે તેને જોવાનું મુશ્કેલ બને.

નિયમિતપણે સ્ટેટમેન્ટ તપાસો: તમારા બેંક સ્ટેટમેન્ટ અને વ્યવહારો પર નજર રાખો. કોઈપણ અજાણી પ્રવૃત્તિની જાણ તરત જ તમારી બેંકને કરો.

કૉલ્સથી સાવચેત રહો: જો કોઈ વ્યક્તિ તમારી બેંકમાંથી હોવાનો દાવો કરે છે અને સંવેદનશીલ માહિતી માંગે છે, તો સાવચેત રહો.બેંકો ફોન પર ભાગ્યે જ PIN અથવા સંપૂર્ણ કાર્ડ નંબર માંગે છે.

સુરક્ષિત **ATM** નો ઉપયોગ કરો: સારી રીતે પ્રકાશિત વિસ્તારોમાં અથવા બેંક શાખાઓ સાથે જોડાયેલા ATM પસંદ કરો, કારણ કે તેમની સાથે ચેષ્ટા થવાની શક્યતા ઓછી હોય છે.

અપડેટ રહો: તમારી જાતને વધુ સારી રીતે સુરક્ષિત રાખવા માટે નવીનતમ કૌભાંડો અને છેતરપિંડીની યુક્તિઓ વિશે માહિતગાર રહો.

યાદ રાખો, જાગ્રત રહેવું અને આ ટીપ્સને અનુસરવાથી તમે ATM કાર્ડ સ્કિમિંગ છેતરપિંડીનો ભોગ બનવાથી બચી શકો છો અને તમારી નાણાકીય બાબતોને સુરક્ષિત રાખી શકો છો.

રિમોટ એક્સેસ છેતરપિંડી

સ્કેમર્સ ગ્રાહકોને સ્ક્રીન-શેરિંગ એપ્લિકેશન ડાઉનલોડ કરવા માટે લલચાવે છે. તેની સાથે, તેઓ તમારા ઉપકરણમાં ઝલક(ચાલાકી) કરે છે, તમારી જાસૂસી કરે છે અને તમારી નાણાકીય માહિતીને સ્વાઇપ કરે છે. પછી, તેઓ તમારા પૈસાથી ખરીદી કરવા જાય છે!

આવા કૌભાંડોથી બચવા માટે, આ ટીપ્સ યાદ રાખો:

કૉલર્સને ચકાસો: તેઓ જે સંસ્થાનું પ્રતિનિધિત્વ કરવાનો દાવો કરે છે તેની અધિકૃત સંપર્ક માહિતી સ્વતંત્ર રીતે જોઈને કૉલરની ઓળખને હંમેશા બે વાર તપાસો.

ઉતાવળમાં નિર્ણય ન લો: દબાણ હેઠળ આવેગજન્ય નિર્ણયો ન લો. ઍક્સેસ આપતા પહેલા અથવા સંવેદનશીલ માહિતી શેર કરતા પહેલા વિચારવા અને ચકાસવા માટે તમારો સમય કાઢીલો.

તમારા ઉપકરણોને સુરક્ષિત કરો: તમારા ઉપકરણોને નવીનતમ સુરક્ષા પેચ સાથે અપડેટ રાખો અને દરેક એકાઉન્ટ માટે મજબૂત, અનન્ય પાસવર્ડ્સનો ઉપયોગ કરો.

તમારી જાતને શિક્ષિત કરો: સામાન્ય કૌભાંડો અને યુક્તિઓ વિશે જાણો જેથી કરીને જ્યારે તેઓ થાય ત્યારે તમે તેમને ઓળખી શકો.

વ્યક્તિગત માહિતીનું રક્ષણ કરો: જ્યાં સુધી તમને વિનંતીની કાયદેસરતા વિશે ખાતરી ન હોય ત્યાં સુધી ફોન, ઇમેઇલ અથવા ઑનલાઇન પર વ્યક્તિગત અથવા નાણાકીય વિગતો શેર કરવા અંગે સાવચેત રહો.

તમારા ડિજિટલ જીવનમાં છૂપાવવાનો પ્રયાસ કરી રહેલા રિમોટ એક્સેસ છેતરપિંડી કરનારાઓ સામે વર્ચ્યુઅલ દરવાજાને લૉક રાખવા માટે સતર્ક રહો.

મહેરબાની કરીને નોંધ કરો - જો તમે કાળી/ખાલી સ્ક્રીન દેખાય, તો કૃપા કરીને તમારી સિસ્ટમ પર કોઈ પણ કાર્યવાહી કરવા યોગ્ય સાથે આગળ વધશો નહીં. આ એક સંકેત હોઈ શકે છે કે તમારી સ્ક્રીન અન્ય લોકો માટે દૃશ્યક્ષમ હોઈ શકે છે.

સિમ સ્વેપ છેતરપિંડી

કલ્પના કરો કે સ્કેમર્સ ફોન ચોરીને ખેંચી રહ્યા છે! તેઓ તમારા હોવાનો ઢોંગ કરે છે, કહે છે કે તેઓ તેમનું સિમ કાર્ડ ખોવાઈ ગયું છે, અને તેમને તમારો નંબર મળી ગયો છે. તેની સાથે, તેઓ તમારી બેંક અથવા ઇમેઇલ જેવા તમારા ઑનલાઇન એકાઉન્ટ્સમાં ક્રેશ થાય છે અને અરાજકતા ફેલાવે છે!

સ્વેપ કૌભાંડ રોકો! નીચેની ટીપ્સ યાદ રાખો.

- SIM કાર્ડ ઓળખની વિગતો શેર કરશો નહીં.
- તમારા ફોનના નેટવર્ક એક્સેસને મોનિટર કરો.

  જો થોડા સમય માટે નેટવર્ક ન હોય, તો ડુપ્લિકેટ SIM તપાસવા માટે તમારા ઓપરેટરનો સંપર્ક કરો.

તમારા ડિજિટલ જીવનમાં ઝલક કરવાનો પ્રયાસ કરતા રિમોટ એક્સેસ છેતરપિંડી કરનારાઓ સામે વર્ચ્યુઅલ ડોર લૉક રાખવા માટે સતર્ક રહો.

કપટપૂર્ણ વ્યવહારની જાણ કેવી રીતે કરવી?

www.axisbank.com ની મુલાકાત લો > સપોર્ટ > 'અમને અહીં પહોંચો' વિભાગ સુધી નીચે સ્ક્રોલ કરો > અમારી સાથે વાત કરો > 'છેતરપિંડી અથવા વિવાદની જાણ કરો' પસંદ કરો > છેતરપિંડીની જાણ કરો > તમારી ક્વેરીનાં ડ્રોપ-ડાઉન સૂચિમાંથી સંબંધિત વિકલ્પ પસંદ કરો> કૉલ પર ક્લિક કરો.

RBIમાં ફરિયાદ નોંધાવવા માટે, https://cms.rbi.org.in ની મુલાકાત લો

ટોલ-ફ્રી નંબર **14448** પર કૉલ કરો (સોમવારથી શુક્રવાર, સવારે 9:30 થી સાંજે 5:15 સુધી, રાષ્ટ્રીય રજાઓ સિવાય).

શારીરિક ફરિયાદ મોકલો: 'સેન્ટ્રલાઈઝ્ડ રિસિપ્ટ એન્ડ પ્રોસેસિંગ સેન્ટર, 4થો માળ, રિઝર્વ બેંક ઑફ ઈન્ડિયા, સેક્ટર -17, સેન્ટ્રલ વિસ્ટા, ચંદીગઢ - 160 017' પર પત્ર/પોસ્ટ. જરૂરી ફોર્મેટ પર વધુ વિગતો માટે કૃપા કરીને https://cms.rbi.org.in ની મુલાકાત લો.

સાયબર ક્રાઈમની જાણ કરવા માટે હેલ્પલાઈન નંબર **155260** અથવા **1930** ડાયલ કરો અથવા નેશનલ સાયબર ક્રાઈમ રિપોર્ટિંગ પોર્ટલ **(www.cybercrime.gov.in)** પર ઘટનાની જાણ કરો.