RBIના નામે વોટ્સએપ પર આવી રહ્યા છે નકલી મેસેજ

લિંક ઓપન કરતા જ ખાતું ખાલી થઇ જશે

આજના ડિજિટલ યુગમાં બેંકિંગ ફ્રોડના કિસ્સાઓ ખૂબ જ ઝડપથી વધી રહ્યા છે. હાલમાં જ સાયબર ગુનેગારો દ્વારા રિઝર્વ બેંક ઓફ ઇન્ડિયાના નામે વોટ્સએપ પર નકલી નોટિસ મોકલીને લોકોને શિકાર બનાવવામાં આવી રહ્યા છે. આ નકલી નોટિસમાં બેંક એકાઉન્ટ બંધ થઈ જશે, કેવાયસી અપડેટ કરવું જરૂરી છે અથવા ખાતામાં શંકાસ્પદ લેવડદેવડ થઈ હોવાનું જણાવી લોકોને ડરાવવામાં આવે છે. ત્યારબાદ નોટિસમાં આપેલી લિંક પર ક્લિક કરવા અથવા કોઈ નંબર પર સંપર્ક કરવા કહેવામાં આવે છે.

મયુર ભુસાવળકર
આઈટી એક્સપર્ટ

સાઇબર સ્કેમર્સ કેવી રીતે ઇન્ટરનેટ યુઝર્સને છેતરે છે?

1. લોગોનો દુરુપયોગ

સ્કેમર્સ તેમના વોટ્સએપ એકાઉન્ટ પર RBI નો અસલી દેખાતો લોગો લગાવે છે, જેથી સામાન્ય માણસ તેને સાચો માની લે.

2. ડર અને ધમકી

મેસેજમાં એવો દાવો કરવામાં આવે છે કે તમારા બેંક એકાઉન્ટમાં શંકાસ્પદ વ્યવહારો થયા છે. જો તમે 3 દિવસમાં વિગતો નહીં આપો, તો તમારું એકાઉન્ટ બંધ કરી દેવામાં આવશે.

3. ખતરનાક ફાઇલો (.ZIP અથવા .APK):

મેસેજની સાથે એક ફાઇલ ડાઉનલોડ કરવા માટે કહેવામાં આવે છે. આ ફાઇલ ખરેખર એક વાયરસ હોય છે. જેવી તમે તેને ડાઉનલોડ કરો, તે તમારા ફોનનો કંટ્રોલ હેકર્સને આપી દે છે.

મેસેજનું 360 ડિગ્રી વિશ્લેષણ

સાઇબર એક્સપર્ટ મયુર ભુસાવળકરે જ્યારે આ મેસેજ નું 360 ડિગ્રી ટેકનીકલ એનાલિસિસ કર્યું, તો તે બાબત સામે આવી કે આ મેસેજ સંપૂર્ણપણે નકલી છે. યુઝર્સને ફસાવવા માટે નવા પ્રકારની .ZIP ફાઇલની યુક્તિઓ વાપરી છે.

1) ખોટો નંબર । રિઝર્વ બેંક ઓફ ઇન્ડિયા ક્યારેય પણ સામાન્ય પર્સનલ વોટ્સએપ (+91) નંબર પરથી ગ્રાહકોને મેસેજ કે નોટિસ મોકલતી નથી.

2) નકલી પ્રોફાઇલ । વિશ્વાસ જીતવા માટે પ્રોફાઇલ પિક્ચરમાં RBI ના સત્તાવાર લોગો નો ઉપયોગ કરવામાં આવ્યો છે.

3) શંકાસ્પદ ફાઇલ । મેસેજ સાથે file_1780044205266.zip નામની ફાઇલ મોકલવામાં આવી છે. આવી ફાઇલોમાં માલવેર અથવા વાયરસ ઉપલબ્ધ હોય છે, જે તમારા ફોન કે કમ્પ્યુટરનો ડેટા ચોરી કરી શકે છે.

4) ડર પેદા કરવો । મેસેજમાં ધમકી આપવામાં આવી છે કે જો 3 દિવસમાં જવાબ નહીં આપો તો તમારું એકાઉન્ટ બંધ થઈ જશે. સ્કેમર્સ હંમેશા તમને ડરાવીને ઉતાવળમાં ભૂલ કરાવવાનો પ્રયાસ કરે છે.

કેસ સ્ટડી

શહેરના યુવાન ચાર્ટર્ડ એકાઉન્ટન્ટ ના મોબાઈલ ઉપર અજાણ્યા મોબાઈલ નંબર પરથી બે પ્રકારના મેસેજ આવ્યા પહેલા મેસેજમાં બેંકના સ્ટેટમેન્ટ ની વાત કરવામાં આવી છે ,બીજા પ્રકારના મેસેજમાં નોટિસ ની વાત કરવામાં આવી છે, બે અલગ અલગ નંબર પરથી આવેલા મેસેજમાં ડીપી પિક્ચર તરીકે આરબીઆઈના લોગોનો ઉપયોગ કરવામાં આવ્યો છે, અને ત્યારબાદ તેમના દ્વારા તે બંને મેસેજ ને ખરાઈ કરવા માટે મને મોકલવામાં આવ્યા.

ભૂલથી આવી કોઈ શંકાસ્પદ લિંક પર ક્લિક કરી દીધું હોય તો ગભરાયા વગર તરત જ આ પગલા લો

1. સોશિયલ મીડિયા અને ઈમેલના પાસવર્ડ બદલો

તમારા મહત્વના એકાઉન્ટ્સ જેવા કે Gmail, WhatsApp, Facebook અને અન્ય પર્સનલ એકાઉન્ટના પાસવર્ડ બદલી નાખો.જો તમારા એકાઉન્ટ્સમાં Two-Factor Authentication (2FA) ચાલુ ન હોય, તો તેને તરત જ સેટિંગ્સમાં જઈને એક્ટિવેટ કરો.

2.ઈન્ટરનેટ તરત જ બંધ કરો

તમારા ફોનનું મોબાઈલ ડેટા અને વાઇ-ફાઇ કનેક્શનને તરત જ બંધ કરી દો.અથવા ફોનને થોડીવાર માટે એરપ્લેન મોડ પર મૂકી દો,આમ કરવાથી હેકર્સ તમારા ફોનમાંથી ઓનલાઇન ડેટા ચોરી શકાશે નહીં અને વાયરસ આગળ કામ કરતો અટકી જશે.

3.અજાણી એપ્સ અને ફાઇલો ડિલીટ કરો

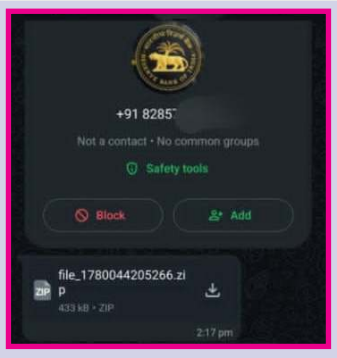
તમારા ફોનના સેટિંગ્સમાં જઈને એપ્લિકેશન લિસ્ટ અથવા ફાઇલ મેનેજર ચેક કરો.જો કોઈ નવી કે અજાણી એપ્લિકેશન ખાસ કરીને તમે ડાઉનલોડ ન કરી હોય તેવી .apk .zip ફાઇલ દેખાય, તો તેને તરત જ Uninstall કરો.

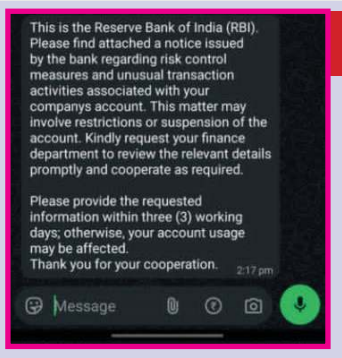
4. બેંક એકાઉન્ટ અને કાર્ડ બ્લોક કરો

જો તમે લિંક પર ક્લિક કરીને બેંકિંગ વિગતો કે પાસવર્ડ ભર્યા હોય, તો તરત જ તમારી બેંકના કસ્ટમર કેરને ફોન કરો.તમારા એટીએમ કાર્ડ, ક્રેડિટ કાર્ડ અને નેટ બેંકિંગ એકાઉન્ટને તાત્કાલિક બ્લોક કરાવો.બેંકિંગ એપ્સના પાસવર્ડ અને UPI પિન બીજા સુરક્ષિત ફોનમાંથી બદલી નાખો.

5. ફોનને સ્કેન કરો અથવા ફેક્ટરી રીસેટ કરો

ગૂગલ પ્લે પ્રોટેક્ટ અથવા કોઈ સારા અને વિશ્વાસુ એન્ટી-વાયરસ સોફ્ટવેર વડે તમારા આખા ફોનને સ્કેન કરો.જો તમને લાગે કે ફોન હજી પણ વિચિત્ર રીતે કામ કરી રહ્યો છે ,જેમ કે જાતે ચાલુ-બંધ થવો કે ગરમ થવો, તો ફોનનો અગત્યનો ડેટા સાચવીને ફોનને ફેક્ટરી રીસેટ કરી દો.





સાયબર સેલમાં ફરિયાદ ક્યાં કરવી?

જો તમારી સાથે નાણાકીય છેતરપિંડી થઈ હોય, તો બિલકુલ સમય બગાડ્યા વિના સાયબર હેલ્પલાઇન નંબર 1930 પર તાત્કાલિક ફોન કરો અથવા સરકારી વેબસાઇટ www.cybercrime.gov.in પર જઈને ઓનલાઇન ફરિયાદ નોંધાવો.

ડિજિટલ ઓળખનું ભવિષ્ય બનશે

ડિજી યાત્રા : હવે માત્ર એરપોર્ટ નહીં, ભારતનું નવું પાસપોર્ટ

એવિએશનથી આગળ વધીને શિક્ષણ, આરોગ્ય અને જાહેર સેવાઓમાં સુરક્ષિત ડિજિટલ ઓળખનો નવો યુગ

ગોપનીયતા, સહમતિ અને ટેક્નોલોજીના સમન્વયથી ભારત બની રહ્યું છે વૈશ્વિક ડિજિટલ ઇનોવેશનનું કેન્દ્ર

YATRA

ભારત ઝડપથી ડિજિટલ પરિવર્તનની દિશામાં આગળ વધી રહ્યું છે અને આ સફરમાં ડિજી યાત્રા એક મહત્વપૂર્ણ માઈલસ્ટોન તરીકે ઉભરી રહી છે. અત્યાર સુધી એરપોર્ટ પર મુસાફરોને ચહેરાની ઓળખના આધારે ઝડપી અને સરળ પ્રવેશ આપતી આ વ્યવસ્થા હવે એવિએશન ક્ષેત્રની બહાર પણ પોતાની પહોંચ વિસ્તારવાની તૈયારીમાં છે. ડિજી યાત્રા ફાઉન્ડેશન હવે તેને માત્ર મુસાફરી માટેની સુવિધા નહીં, પરંતુ સમગ્ર દેશ માટે એક વિશ્વસનીય ડિજિટલ આઈડેન્ટિટી પ્લેટફોર્મ તરીકે વિકસાવવા માંગે છે. આ પ્લેટફોર્મ બાયોમેટ્રિક્સ, વેરિફાયેબલ ક્રેડેન્શિયલ્સ અને ઓપન સ્ટાન્ડર્ડ્સના આધારે કાર્ય કરે છે, જેના કારણે વ્યક્તિની ઓળખ સુરક્ષિત, સરળ અને વિશ્વસનીય રીતે ચકાસી શકાય છે. ડિજી યાત્રાની સૌથી મોટી વિશેષતા તેની પ્રાઈવસી-બાય-ડિઝાઈન પદ્ધતિ છે. વપરાશકર્તાની સહમતિ વિના કોઈપણ માહિતીનો ઉપયોગ થતો નથી, જેના કારણે ડેટાની સુરક્ષા અને વ્યક્તિગત ગોપનીયતા જળવાઈ રહે છે. આ મોડેલ ભવિષ્યમાં શિક્ષણ, આરોગ્ય, સરકારી સેવાઓ અને મોટા જાહેર કાર્યક્રમોમાં પણ ઉપયોગી બની શકે છે. તાજેતરમાં ભારત AI ઈમ્પેક્ટ સમિટમાં ડિજી યાત્રાનો સફળ ઉપયોગ કરવામાં આવ્યો હતો, જે એવિએશન બહારના ક્ષેત્રોમાં તેની ઉપયોગિતાનું પ્રથમ મોટું ઉદાહરણ બન્યું.

ડિજી યાત્રા શું છે?

ડિજી યાત્રા એ ફેશિયલ રેકોગ્નિશન (ચહેરાની ઓળખ) આધારિત ડિજિટલ સિસ્ટમ છે, જે મુસાફરોને એરપોર્ટ પર કાગળરહિત અને ઝડપી પ્રવેશની સુવિધા આપે છે. મુસાફરની ઓળખ એકવાર ચકાસ્યા બાદ વિવિધ ચેકપોઈન્ટ પર બોર્ડિંગ પાસ અથવા ઓળખપત્ર બતાવવાની જરૂરિયાત ઘટે છે. આથી સમયની બચત થાય છે અને મુસાફરીનો અનુભવ વધુ સરળ બને છે.

ગોપનીયતા અને સુરક્ષા પર ખાસ ભાર

ડિજી યાત્રા 'પ્રાઈવસી બાય ડિઝાઇન' સિદ્ધાંત પર કાર્ય કરે છે. વપરાશકર્તાની સ્પષ્ટ મંજૂરી વિના કોઈપણ વ્યક્તિગત માહિતીનો ઉપયોગ થતો નથી. બાયોમેટ્રિક ડેટાનું સુરક્ષિત સંચાલન અને ડેટા શેરિંગ પર નિયંત્રણ હોવાથી વપરાશકર્તાની ગોપનીયતા જળવાઈ રહે છે. આ મોડેલને કારણે ડિજી યાત્રા વિશ્વસનીય ડિજિટલ ઓળખ પ્લેટફોર્મ તરીકે ઉભરી રહી છે.

એરપોર્ટથી આગળ વધતી ડિજી યાત્રા

ડિજી યાત્રાનો ઉપયોગ હવે માત્ર હવાઈ મુસાફરી પૂરતો મર્યાદિત રહેશે નહીં. ભવિષ્યમાં શિક્ષણ, આરોગ્ય, સરકારી સેવાઓ, કોન્ફરન્સ, એક્ઝિબિશન અને મોટા જાહેર કાર્યક્રમોમાં પણ તેની મદદથી ઓળખ ચકાસણી સરળ અને ઝડપી બની શકે છે. આથી ડિજિટલ સેવાઓ વધુ સુલભ અને કાર્યક્ષમ બનવાની શક્યતા છે.

ડિજી યાત્રાની મુખ્ય વિશેષતાઓ

- ચહેરાની ઓળખ આધારિત ઝડપી પ્રવેશ
- કાગળરહિત અને સંપર્કરહિત પ્રક્રિયા
- વપરાશકર્તાની સહમતિ આધારિત ડેટા ઉપયોગ
- સુરક્ષિત બાયોમેટ્રિક વેરિફિકેશન
- ઓપન સ્ટાન્ડર્ડ્સ અને ડિજિટલ ક્રેડેન્શિયલ્સનો ઉપયોગ
- ભવિષ્યમાં શિક્ષણ, આરોગ્ય-સરકારી સેવાઓમાં ઉપયોગની સંભાવના
- આંતરરાષ્ટ્રીય ડિજિટલ ટ્રાવેલ ઇકોસિસ્ટમ સાથે જોડાવાની તૈયારી
- કરોડો મુસાફરો દ્વારા અપનાવવામાં આવેલી વિશ્વસનીય વ્યવસ્થા
- ડિજી યાત્રા માત્ર એક ટેક્નોલોજી પ્લેટફોર્મ નથી તે ભારતના ડિજિટલ ભવિષ્યની એવી ઝલક છે, જ્યાં ઓળખ, સુરક્ષા અને સુવિધા એકસાથે આગળ વધે છે.

સોશિયલ મીડિયા માર્કેટિંગની દોડમાં સંગીતના હક્કો બની રહ્યા છે વિવાદનું કેન્દ્ર

રીલ્સનો રણકાર અને કૉપિરાઇટનો કહેર

ઇન્સ્ટાગ્રામ અને અન્ય સોશિયલ મીડિયા પ્લેટફોર્મ પર રીલ્સ આજે બ્રાન્ડ પ્રમોશનનું સૌથી શક્તિશાળી હથિયાર બની ગઈ છે. પરંતુ લોકપ્રિય ગીતોનો ઉપયોગ કરીને બનાવવામાં આવતી રીલ્સ હવે કાનૂની વિવાદોને જન્મ આપી રહી છે. સંગીત કંપનીઓ દાવો કરી રહી છે કે અનેક બ્રાન્ડ્સ અને ઇન્ફ્લુએન્સર્સ યોગ્ય લાઇસન્સ લીધા વગર ગીતોનો વ્યાવસાયિક ઉપયોગ કરે છે, જેના કારણે કૉપિરાઇટ ભંગના કેસોમાં વધારો થયો છે. તાજેતરમાં અનેક જાણીતી કંપનીઓ અને બ્રાન્ડ્સ સામે થયેલા દાવાઓએ સમગ્ર ડિજિટલ માર્કેટિંગ ઉદ્યોગને ચેતવણી આપી છે. નિષ્ણાતોના જણાવ્યા અનુસાર, સોશિયલ મીડિયા પ્લેટફોર્મ પર ઉપલબ્ધ ગીતોનો ઉપયોગ વ્યક્તિગત અને મનોરંજન માટેની પોસ્ટ્સમાં કરવો અને વ્યાવસાયિક અથવા વ્યાપારી હેતુ માટે તેનો ઉપયોગ કરવો - બંને બાબતોમાં કાનૂની રીતે તફાવત છે.

બ્રાન્ડ પ્રમોશનની નવી મુશ્કેલી

હજારો કરોડ રૂપિયાની રોયલ્ટી દાવ પર

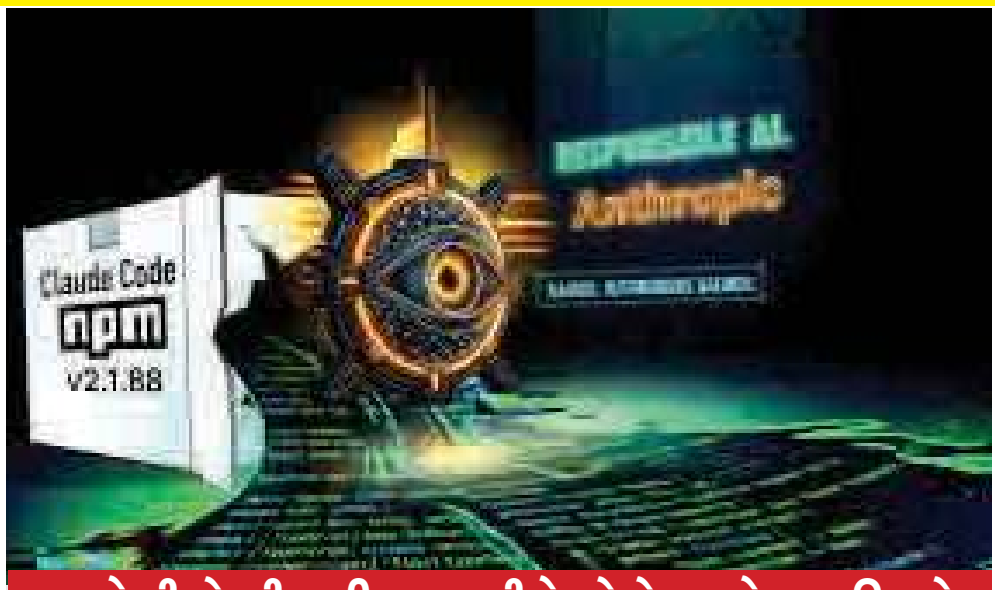
સંગીત ઉદ્યોગના નિષ્ણાતોના મતે, લોકપ્રિય ગીતો રીલ્સની પહોંચ અને એન્ગેજમેન્ટમાં નોંધપાત્ર વધારો કરે છે, પરંતુ તેના બદલામાં સર્જકો અને સંગીત કંપનીઓને મળવી જોઈએ એવી રોયલ્ટી ઘણીવાર ચૂકવાતી નથી. સંગીત ઉદ્યોગને દર વર્ષે હજારો કરોડ રૂપિયાનું નુકસાન થતું હોવાનું માનવામાં આવે છે. હવે કોપિરાઇટ કાયદાનું કડક પાલન, યોગ્ય લાઇસન્સિંગ અને ડિજિટલ કન્ટેન્ટ સર્જકોમાં જાગૃતિ લાવવી સમયની માંગ બની ગઈ છે. ડિજિટલ યુગમાં કન્ટેન્ટની સફળતા માત્ર સર્જનાત્મકતા પર નહીં, પરંતુ કાયદાકીય જવાબદારી પર પણ નિર્ભર છે–અને રીલ્સની દુનિયામાં આ હકીકત હવે વધુ સ્પષ્ટ બની રહી છે.

AI માત્ર ટેક્નોલોજી નહીં, પરંતુ સમાજના વિશ્વાસ સાથે જોડાયેલો મુદ્દો

AIનો યુગ । સલાહ મશીનો આપે, વિશ્વાસ કોણ નક્કી કરે?

ડિજિટલ ગુરુઓનો ઉદય : જવાબો ઝડપથી મળે, પરંતુ જવાબદારી કોની?

એક સમય હતો જ્યારે કાનૂની સલાહ માટે વકીલ, આરોગ્ય માટે ડૉક્ટર અને અભ્યાસ માટે શિક્ષકનો સહારો લેવાતો. આજે AI ચેટબોટ્સ સેકન્ડોમાં પ્રશ્નોના જવાબ આપે છે, લેખ લખે છે, રોકાણ અંગે સૂચનો આપે છે અને જીવનના મહત્વપૂર્ણ નિર્ણયો પર માર્ગદર્શન પણ આપે છે. પરંતુ જ્યારે લાખો લોકો AI પર વિશ્વાસ મૂકવા લાગે, ત્યારે સૌથી મોટો પ્રશ્ન ઊભો થાય છે–જો AI ખોટી સલાહ આપે તો તેની જવાબદારી કોણ લેશે?AIની ઝડપ અને સુવિધા તેને લોકપ્રિય બનાવી રહી છે, પરંતુ તેની પાછળ રહેલા અલ્ગોરિધમ્સ ક્યારેક ખોટી અથવા ભ્રામક માહિતી પણ રજૂ કરી શકે છે. સામાન્ય વપરાશકર્તા માટે સાચું અને ખોટું અલગ પાડવું હંમેશા સરળ નથી. પરિણામે, AI માત્ર ટેક્નોલોજી નહીં, પરંતુ સમાજના વિશ્વાસ સાથે જોડાયેલો મુદ્દો બની ગયો છે.



AI સેફ્ટી કોડની જરૂરિયાત: નવી ટેક્નોલોજી માટે નવા નિયમો

વિશ્વભરમાં સરકારો અને નિયમનકારી સંસ્થાઓ AI માટે સુરક્ષા માળખું તૈયાર કરવાની દિશામાં આગળ વધી રહી છે. નિષ્ણાતો માને છે કે શિક્ષણ, આરોગ્ય, કાનૂની અને નાણાકીય ક્ષેત્રોમાં ઉપયોગ થતી AI સેવાઓ માટે સ્પષ્ટ માર્ગદર્શિકા અને જવાબદારીના ધોરણો હોવા જોઈએ. AI કંપનીઓ માટે પારદર્શિતા, સ્રોતોની ચકાસણી અને જોખમોની સ્પષ્ટ જાણકારી આપવી જરૂરી બની રહી છે. જો AI લોકોના જીવનને અસર કરતી સલાહ આપે છે, તો તેના પર વિશ્વાસ સ્થાપિત કરવા માટે માત્ર ટેક્નોલોજી પૂરતી નથી–મજબૂત નિયમન, નૈતિકતા અને જાહેર જવાબદારી પણ એટલી જ જરૂરી છે. AIનો પ્રશ્ન હવે માત્ર "તે શું કરી શકે?" એટલો રહ્યો નથી. સાચો પ્રશ્ન એ છે કે "તે જે કહે છે તેના પર વિશ્વાસ કેટલો કરવો?" અને તેનો જવાબ ટેક્નોલોજી કરતાં વધુ સમાજ, સરકાર અને ઉદ્યોગના સંયુક્ત પ્રયાસોમાં છુપાયેલો છે.