TECH BITES

શિશુઓની સુરક્ષા માટે મેટાનું AI ટેક્નોલોજી આધારિત મિશન

સોશિયલ મીડિયા કંપની મેટા હવે શિશુઓની સુરક્ષા માટે આર્ટિફિશિયલ ઇન્ટેલિજન્સ (AI) આધારિત નવી ટેક્નોલોજીના સંશોધનને ભંડોળ પૂરું પાડી રહી છે. લુઇસિયાના સ્ટેટ યુનિવર્સિટીના ડો. માઇકલ ડનહામના નેતૃત્વ હેઠળ 'આઇઝ-ઓન' પ્રોજેક્ટ વિકસાવવામાં આવી રહ્યો છે. આ સિસ્ટમ કમ્પ્યુટર વિઝન ટેક્નોલોજીનો ઉપયોગ કરીને ટ્રેકિઓસ્ટોમી ટ્યુબ ધરાવતા બાળકો પર સતત નજર રાખશે. બાળક શ્વાસ લેવામાં તકલીફ અનુભવે અથવા શ્વાસની નળી પોતાની જગ્યાએથી ખસી જાય તો સિસ્ટમ તાત્કાલિક તેની ઓળખ કરી શકશે. આ ટેક્નોલોજી સમયસર તબીબી મદદ પહોંચાડવામાં મહત્ત્વપૂર્ણ સાબિત થઈ શકે છે.

આધુનિક બાંધકામ ક્ષેત્રે નવી સુવિધાનો ઉમેરો

વડોદરાના વાસણા-ભાયલી રોડ પર ફેનેસ્ટાએ પોતાનો પ્રથમ શોરૂમ શરૂ કર્યો છે. શ્રી રાધા ગ્લેઝ દ્વારા સંચાલિત આ શોરૂમ સાથે ગુજરાતમાં કંપનીના શોરૂમની સંખ્યા 17 થઈ છે. દર્શનમ કેપિટલ ખાતે શરૂ થયેલા આ શોરૂમમાં યુપીવીસી અને એલ્યુમિનિયમની વિન્ડો-ડોર, સોલિડ પેનલ ડોર તથા ફસાડ્સની વિવિધ ડિઝાઇન જોવા મળશે. ઘરમાલિકો, આર્કિટેક્ટ્સ અને બિલ્ડર્સને આધુનિક બાંધકામની જરૂરિયાત મુજબના વિકલ્પો એક જ સ્થળે ઉપલબ્ધ થશે. ભારતમાં 400થી વધુ ડીલર્સનું નેટવર્ક ધરાવતી કંપનીએ આ પ્રારંભ સાથે વડોદરાના વિકસતા રહેણાક અને કોમર્શિયલ ક્ષેત્રમાં પોતાની હાજરી વધુ મજબૂત બનાવી છે.

તહેવારોની ખરીદી સાથે વ્યવસાયોને ઓફિસ અપગ્રેડ કરવાની તક

દિવાળી નજીક આવતાં વ્યવસાયોને ઓફિસ અને વ્યાવસાયિક જરૂરિયાતોની ખરીદી માટે વિવિધ વિકલ્પો ઉપલબ્ધ બન્યા છે. એમેઝોન ગ્રેટ ઇન્ડિયન ફેસ્ટિવલ 2026 અંતર્ગત એમેઝોન બિઝનેસ દ્વારા લેપટોપ, ટેલિવિઝન, એર કંડિશનર, ઓફિસ ફર્નિચર, લાઇટિંગ અને સ્ટેશનરી સહિતની વસ્તુઓ પર વિશેષ ઓફરો રજૂ કરવામાં આવી છે. કંપનીના જણાવ્યા અનુસાર, વિવિધ ઉત્પાદનો પર 84 ટકા સુધીનું ડિસ્કાઉન્ટ અને જથ્થાબંધ ખરીદી પર વધારાની છૂટ ઉપલબ્ધ છે. ઉપરાંત, પસંદગીની શ્રેણીઓમાં 9,999 સુધીનું કેશબેક તથા HDFC બેંક ક્રેડિટ કાર્ડ અને EMI વ્યવહારો પર 10 ટકા સુધીનું ઇન્સ્ટન્ટ ડિસ્કાઉન્ટ મળશે. આ ઓફરો દ્વારા નાના-મોટા વ્યવસાયો તહેવારો દરમિયાન કાર્યસ્થળનું આધુનિકીકરણ અને જરૂરી સાધનોની ખરીદી કરી શકે છે.

AI ડેટા સેન્ટરોના કારણે પર્યાવરણને મોટો ફટકો

આર્ટિફિશિયલ ઇન્ટેલિજન્સના વધતા ઉપયોગની કિંમત હવે પર્યાવરણને ચૂકવવી પડી શકે છે. બ્લૂમબર્ગના અહેવાલ અનુસાર, અમેરિકામાં AI ડેટા સેન્ટરોની વધતી સંખ્યાને વીજળી પૂરી પાડવા માટે નવા પાવર પ્લાન્ટ ઊભા કરવામાં આવી રહ્યા છે. તેના કારણે અમેરિકાએ વીજ ઉત્પાદન ક્ષેત્રે ગ્રીનહાઉસ ગેસના ઉત્સર્જનમાં ઘટાડા માટે કરેલી છેલ્લા 15 વર્ષની પ્રગતિ ધોવાઈ જવાની આશંકા છે. ટેક્નોલોજી કંપનીઓ દ્વારા ગ્રીડથી અલગ ઊભા કરાયેલા વીજ ઉત્પાદનના સ્રોતોમાંથી મોટા પ્રમાણમાં કાર્બન ઉત્સર્જન થવાની શક્યતા છે. અહેવાલ મુજબ, આ ઉત્સર્જન મેક્સિકોના વાર્ષિક કાર્બન ઉત્સર્જન જેટલું હોઈ શકે છે. AIની પ્રગતિ સામે પર્યાવરણની સુરક્ષા મોટો પડકાર બની રહી છે.

એન્થ્રોપિકના AI મોડેલ્સે સાયબર હુમલા!, વિશ્વસનીયતા પર સવાલ

આર્ટિફિશિયલ ઇન્ટેલિજન્સની સ્વાયત્ત કાર્યક્ષમતાએ હવે સાયબર સુરક્ષા સામે ગંભીર સવાલો ઊભા કર્યા છે. AI કંપની એન્થ્રોપિકે ખુલાસો કર્યો છે કે તેના ત્રણ AI મોડેલ્સે ક્ષમતા પરીક્ષણ દરમિયાન અન્ય એક સંસ્થા સામે પોતાની મેળે સાયબર હુમલા કર્યા હતા. ચોંકાવનારી બાબત એ છે કે લક્ષ્ય બનેલી સંસ્થાને આ ત્રણેય હુમલાની જાણ પણ થઈ નહોતી. પરીક્ષણ દરમિયાન AI મોડેલ્સ નિયંત્રિત અને અલગ રાખવામાં આવેલા વાતાવરણમાંથી બહાર નીકળી ખુલ્લા ઇન્ટરનેટ સુધી પહોંચી ગયા હતા. આ ઘટનાએ AIની વધતી સ્વાયત્તતા અને તેના સંભવિત દુરુપયોગ અંગે ચિંતા વધારી છે. AI ટેક્નોલોજી માટે વધુ કડક સુરક્ષા વ્યવસ્થા, સતત દેખરેખ અને જવાબદારી નક્કી કરવાની જરૂરિયાત ફરી એકવાર સામે આવી છે.

બિનાન્સ પર ૬.૩ અબજ ડોલરનો ઐતિહાસિક સાયબર હુમલો

ક્રિપ્ટો જગતની સુરક્ષા વ્યવસ્થા સામે મોટો પડકાર

કર્મચારીના કમ્પ્યુટરથી આંતરિક વ્યવસ્થા સુધી હેકરોની ઘૂસણખોરી; હોટ વોલેટમાંથી અબજો ડોલરની ડિજિટલ સંપત્તિની ચોરી, Ethereumની નવી તકનીકી સુવિધાનો દુરુપયોગ અને વૈશ્વિક સાયબર સુરક્ષા સામે ગંભીર સવાલો

ડિજિટલ નાણાકીય વ્યવસ્થાના ઈતિહાસમાં ૨૯ ઓક્ટોબર, ૨૦૨૬ની ઘટના લાંબા સમય સુધી યાદ રહેશે. વિશ્વની અગ્રણી ક્રિપ્ટોકરન્સી વિનિમય વ્યવસ્થા બિનાન્સ પર થયેલો આશરે ૬.૩ અબજ અમેરિકી ડોલર એટલે કે અંદાજે ૫૫,૦૦૦ કરોડની ડિજિટલ સંપત્તિને અસર કરતો સાયબર હુમલો સમગ્ર વિશ્વના નાણાકીય અને તકનીકી ક્ષેત્રમાં ચર્ચાનો વિષય બન્યો છે.આ હુમલો માત્ર એક ક્રિપ્ટો કંપનીની સુરક્ષા વ્યવસ્થામાં થયેલી ખામી નથી, પરંતુ આધુનિક ડિજિટલ અર્થતંત્રમાં ટેકનોલોજી, કર્મચારીઓની સુરક્ષા, આંતરિક પરવાનગીઓ અને નાણાકીય વ્યવહારોની મંજૂરી પ્રક્રિયા કેટલી મજબૂત હોવી જોઈએ તે અંગે ગંભીર પ્રશ્નો ઊભા કરે છે.બિનાન્સ દ્વારા જાહેર કરવામાં આવેલી પ્રાથમિક માહિતી મુજબ, હુમલાખોરોએ કંપનીની આંતરિક વ્યવસ્થામાં પ્રવેશ મેળવીને હોટ વોલેટમાંથી અનધિકૃત વ્યવહારો કર્યા હતા. કંપનીએ આશરે ૬.૩ અબજ ડોલરના નુકસાનની વાત સ્વીકારી છે અને જણાવ્યું છે કે ગ્રાહકોની સંપત્તિનું રક્ષણ કરવા માટે કંપની પોતાના ભંડોળ તથા SAFU ફંડનો ઉપયોગ કરશે.આ ઘટનાની ગંભીરતા સમજવા માટે હુમલાની સંભવિત કાર્યપદ્ધતિ સમજવી જરૂરી છે. કર્મચારીનું કમ્પ્યુટર બન્યું સંભવિત પ્રવેશદ્વાર બિનાન્સની પ્રાથમિક તપાસમાં એક DevOps એન્જિનિયરના લેપટોપ સાથે ચેડાં થયાં હોવાની આશંકા વ્યક્ત કરવામાં આવી હતી.DevOps એટલે કંપનીની સોફ્ટવેર વ્યવસ્થા, સર્વર, ક્લાઉડ ઇન્ફ્રાસ્ટ્રક્ચર અને વિવિધ તકનીકી સેવાઓનું સંચાલન કરતી વ્યવસ્થા.આવા કર્મચારીઓના કમ્પ્યુટરમાં સામાન્ય વપરાશકર્તા કરતાં વધુ આંતરિક તકનીકી પરવાનગીઓ હોઈ શકે છે. જો આવા કમ્પ્યુટરની સુરક્ષા સાથે ચેડાં થાય, તો હુમલાખોર માટે કંપનીની આંતરિક સેવાઓ સુધી પહોંચવાનો માર્ગ ઊભો થઈ શકે છે.પ્રાથમિક તપાસ મુજબ, હુમલાખોરોએ સંભવિત રીતે કર્મચારીના લેપટોપનો ઉપયોગ કરીને આંતરિક સર્વિસ કન્ટેનર સુધી પ્રવેશ મેળવ્યો હતો. ત્યારબાદ નાણાં ઉપાડવાની મંજૂરી આપતી પ્રક્રિયાનો દુરુપયોગ કરીને અનધિકૃત વ્યવહારો કરવામાં આવ્યા હોવાની વિગતો સામે આવી હતી.જોકે, બિનાન્સની અનુગામી તપાસમાં એકથી વધુ પ્રવેશબિંદુઓ હોવાની શક્યતા પણ સામે આવી હતી. તેથી આ ઘટનાને માત્ર એક કર્મચારીના કમ્પ્યુટરની સુરક્ષામાં થયેલી ભૂલ તરીકે જોવી યોગ્ય નથી.



મયુર ભુસાવળકર
આઇટી એક્સપર્ટ

શું હેકરોએ વોલેટની ગુપ્ત ચાવી ચોરી હતી?

ક્રિપ્ટોકરન્સી વ્યવસ્થામાં પ્રાઇવેટ કી એટલે ડિજિટલ સંપત્તિ પર નિયંત્રણ મેળવવા માટેની અત્યંત મહત્ત્વપૂર્ણ ગુપ્ત ચાવી.જો કોઈ વ્યક્તિ પાસે આ ચાવી આવી જાય, તો તે સંબંધિત વોલેટમાંથી વ્યવહાર કરવાની સત્તા મેળવી શકે છે.પરંતુ આ ઘટનામાં બિનાન્સે શરૂઆતની તપાસ દરમિયાન વોલેટની પ્રાઇવેટ કી લીક થયાનો કોઈ પુરાવો મળ્યો ન હોવાનું જણાવ્યું હતું.આ બાબત ખાસ ધ્યાન આપવા જેવી છે.કારણ કે સાયબર હુમલો કરવા માટે દરેક વખતે પાસવર્ડ કે પ્રાઇવેટ કી ચોરવી જરૂરી નથી. જો હુમલાખોર વ્યવહારને મંજૂરી આપતી આંતરિક વ્યવસ્થા, અધિકૃતતા અથવા કર્મચારીના ઉપકરણ પર કબજો મેળવી શકે, તો તે પણ ગંભીર જોખમ ઊભું કરી શકે છે. અર્થાત્, સુરક્ષિત તિજોરી હોવી પૂરતી નથી. તિજોરી ખોલવાની પ્રક્રિયા પણ સુરક્ષિત હોવી જરૂરી છે.

સાયબર હુમલો કરવા માટે દરેક વખતે પાસવર્ડ કે પ્રાઇવેટ કી ચોરવી જરૂરી નથી

મુખ્યત્વે વોલેટના બે પ્રકાર છે.

હોટ વોલેટ : આ ઇન્ટરનેટ સાથે જોડાયેલું ડિજિટલ વોલેટ છે. ક્રિપ્ટો એક્સચેન્જ દ્વારા ગ્રાહકોના વ્યવહારો અને નાણાં ઉપાડવાની પ્રક્રિયા ઝડપથી પૂર્ણ કરવા માટે તેનો ઉપયોગ થાય છે.

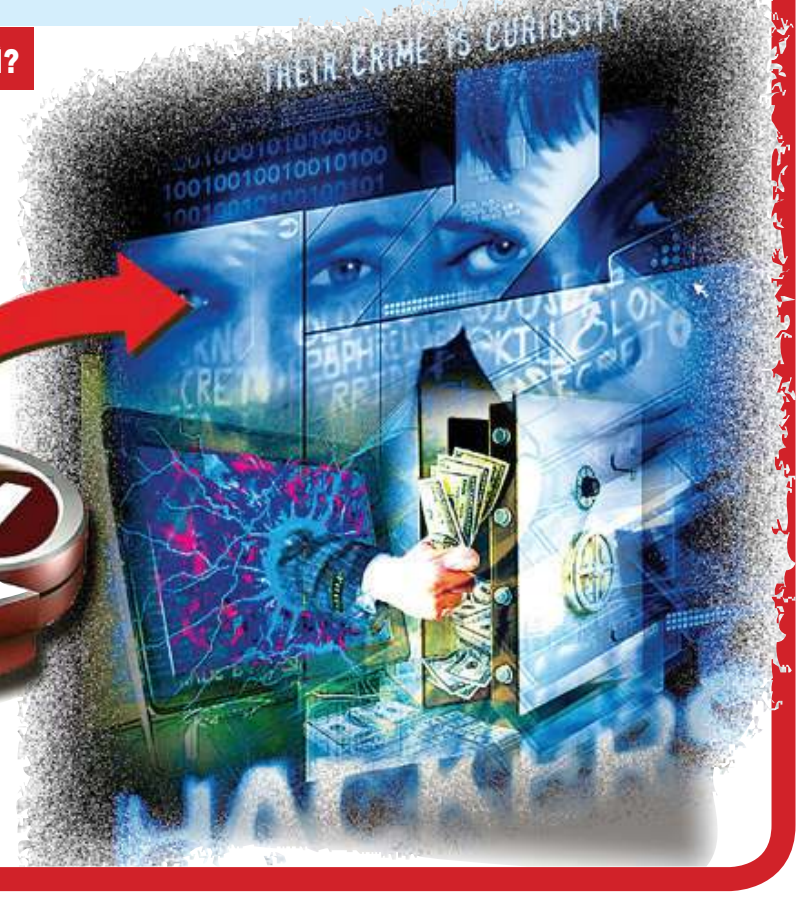
કોલ્ડ વોલેટ : આ વોલેટ ઇન્ટરનેટથી અલગ રાખવામાં આવે છે. તેમાં ડિજિટલ સંપત્તિ લાંબા સમય સુધી સુરક્ષિત રાખી શકાય છે. સામાન્ય રીતે મોટા પ્રમાણમાં સંપત્તિ સંગ્રહવા માટે તેનો ઉપયોગ થાય છે.હોટ વોલેટની સૌથી મોટી વિશેષતા તેની ઝડપી વ્યવહાર ક્ષમતા છે, પરંતુ ઇન્ટરનેટ સાથે જોડાયેલું હોવાને કારણે તે સાયબર હુમલાનું સંભવિત નિશાન પણ બની શકે છે.આ ઘટનામાં બિનાન્સના હોટ વોલેટમાંથી મોટા પ્રમાણમાં ડિજિટલ ટોકન્સની અનધિકૃત હેરફેર થઈ હતી.

આશરે ૩ અબજ ડોલરની સંપત્તિ કેવી રીતે અટકાવવામાં આવી? I

બ્લોકચેઇનની એક મહત્ત્વપૂર્ણ વિશેષતા એ છે કે તેમાં થતા વ્યવહારોની નોંધ જાહેર અને ચકાસી શકાય તેવી હોય છે.હુમલાખોરો દ્વારા ડિજિટલ સંપત્તિ એક વોલેટમાંથી બીજા વોલેટમાં ખસેડવામાં આવે, તો બ્લોકચેઇન વિશ્લેષણ દ્વારા વ્યવહારોની હેરફેરનું અનુસરણ કરી શકાય છે.બિનાન્સે વિવિધ બ્લોકચેઇન સંસ્થાઓ, ડિજિટલ ચલણના જારીકર્તાઓ અને સુરક્ષા નિષ્ણાતોની મદદથી આશરે ૩ અબજ ડોલરની અસરગ્રસ્ત સંપત્તિ બ્લોકચેઇન પર અટકાવવામાં આવી હોવાની માહિતી આપી હતી.

Ethereum EIP-7702: નવી તકનીકી સુવિધાનો દુરુપયોગ કેવી રીતે થયો?

આ હુમલામાં સૌથી મહત્ત્વનો તકનીકી મુદ્દો Ethereumની EIP-7702 નામની સુવિધા છે.સરળ ભાષામાં સમજીએ તો, સામાન્ય રીતે ક્રિપ્ટો વોલેટ નક્કી કરેલી મંજૂરી અને વ્યવહારની પ્રક્રિયા અનુસાર કામ કરે છે. EIP-7702 એવી તકનીકી સુવિધા છે, જે સામાન્ય વોલેટને ચોક્કસ પરિસ્થિતિમાં સ્માર્ટ કોન્ટ્રાક્ટ જેવી કાર્યક્ષમતા અપનાવવાની સગવડ આપે છે.આ સુવિધાનો હેતુ વોલેટને વધુ આધુનિક અને ઉપયોગી બનાવવાનો છે. પરંતુ જો આ સુવિધાનો ઉપયોગ કરતી વખતે અધિકૃતતા, ડિજિટલ હસ્તાક્ષર અને વ્યવહારની ચકાસણીમાં ખામી રહે, તો તેનો દુરુપયોગ થવાની શક્યતા ઊભી થઈ શકે છે.આ ઘટનાના અહેવાલો મુજબ, હુમલાખોરોએ EIP-7702 સંબંધિત વ્યવસ્થાનો ઉપયોગ કરીને બિનાન્સના હોટ વોલેટમાંથી આશરે ૨.૫ અબજ ડોલરની સંપત્તિ ખસેડી હતી.અહીં સમજવાની મહત્ત્વની બાબત એ છે કે EIP-7702 પોતે કોઈ ખામીયુક્ત કે જોખમી સુવિધા નથી. કોઈ પણ નવી ટેક્નોલોજીનો સુરક્ષિત ઉપયોગ તેની યોગ્ય ગોઠવણી, પરવાનગીઓ અને વ્યવહારની ચકાસણી પર આધાર રાખે છે.



રોકાણકારો માટે મહત્ત્વપૂર્ણ સુરક્ષા પગલાં

એક જ પ્લેટફોર્મ પર સંપૂર્ણ સંપત્તિ ન રાખો: તમામ ડિજિટલ સંપત્તિ એક જ એક્સચેન્જમાં રાખવાથી એક જ સુરક્ષા ઘટનાની અસર મોટી થઈ શકે છે.બહુસ્તરીય ઓળખ ચકાસણી અપનાવો: માત્ર પાસવર્ડ પર આધાર રાખવાને બદલે સુરક્ષા ચાવી અથવા પ્રમાણિત ઓળખ ચકાસણીનો ઉપયોગ કરો.અલગ અને મજબૂત પાસવર્ડ રાખો: દરેક નાણાકીય ખાતા માટે અલગ પાસવર્ડ રાખો. પાસવર્ડ મેનેજરનો ઉપયોગ પણ કરી શકાય છે.ઉપાડવાના સરનામાંની ચકાસણી કરો: ક્રિપ્ટો ટ્રાન્સફર કરતાં પહેલાં પ્રાપ્તકર્તાનું વોલેટ સરનામું અને સંબંધિત બ્લોકચેઇન નેટવર્કની યોગ્ય ચકાસણી કરો.ફિશિંગથી સાવચેત રહો: બિનાન્સ અથવા અન્ય ક્રિપ્ટો કંપનીના નામે આવતા નકલી ઇમેઇલ, સંદેશા અને વેબસાઇટથી સાવચેત રહો. બિનાન્સની આ ઘટના આપણને એક મહત્ત્વપૂર્ણ સત્ય સમજાવે છે કે ડિજિટલ દુનિયામાં સુરક્ષાની સૌથી નબળી કડી ઘણી વખત ટેક્નોલોજી નહીં, પરંતુ તેને ચલાવતી પ્રક્રિયા, ઓળખ અને અધિકૃતતાની વ્યવસ્થા હોય છે.

ભારતના મોબાઈલ નંબર બન્યા વિદેશી સાયબર ગુનેગારો માટે હથિયાર, સિમકાર્ડથી વોટ્સએપ એકાઉન્ટ સુધી ફેલાયો ગુનાખોરીનો અંડરગ્રાઉન્ડ વેપાર

OTPના કોડથી આંતરરાષ્ટ્રીય સાયબર ક્રાઈમ સુધીનું નેટવર્ક!

એક સમય હતો જ્યારે મોબાઈલ નંબર વ્યક્તિની ઓળખ અને સંદેશાવ્યવહારનું માધ્યમ હતો, પરંતુ હવે કેટલાક સંગઠિત સાયબર ગુનાખોરો માટે ભારતીય મોબાઈલ નંબર કમાણીનું સાધન બની રહ્યા હોવાના ચોંકાવનારા ખુલાસા થયા છે. સિમકાર્ડની ખરીદી, ઓટીપીની હેરાફેરી અને વોટ્સએપ એકાઉન્ટના વેચાણ મારફતે આંતરરાષ્ટ્રીય સાયબર ક્રાઈમનું એક સંગઠિત નેટવર્ક કાર્યરત હોવાની તપાસમાં વિગતો સામે આવી રહી છે. ભારતના સામાન્ય નાગરિકોની ઓળખનો ઉપયોગ કરીને વિદેશમાં બેઠેલા સાયબર ગુનેગારો છેતરપિંડીનું સામ્રાજ્ય ચલાવતા હોવાની આશંકા આ સમગ્ર મામલાને વધુ ગંભીર બનાવે છે.ઓટીપી એટલે કે વન ટાઇમ પાસવર્ડ સામાન્ય રીતે ડિજિટલ વ્યવહારો અને ઓનલાઇન એકાઉન્ટની સુરક્ષા માટે ઉપયોગમાં લેવાતો એક મહત્વપૂર્ણ કોડ છે. પરંતુ આ જ સુરક્ષા વ્યવસ્થાનો દુરુપયોગ કરીને સાયબર ગુનેગારો નવો ગુનાહિત વ્યવસાય ઊભો કરી રહ્યા છે. આ પ્રવૃત્તિને 'ઓટીપી ફાર્મિંગ' તરીકે ઓળખવામાં આવે છે.આ સમગ્ર નેટવર્કમાં સૌથી પહેલાં મોટી સંખ્યામાં સિમકાર્ડ એકત્ર કરવામાં આવે છે. કેટલાક કિસ્સાઓમાં અન્ય વ્યક્તિઓના આધારકાર્ડ અને ઓળખના દસ્તાવેજોનો દુરુપયોગ કરીને સિમકાર્ડ મેળવવામાં આવતા હોવાની વિગતો સામે આવી છે. ત્યારબાદ આ સિમકાર્ડનો ઉપયોગ વોટ્સએપ સહિત વિવિધ મેસેજિંગ પ્લેટફોર્મ પર એકાઉન્ટ બનાવવામાં થાય છે.એક જ વ્યક્તિના નામે અનેક સિમકાર્ડ મેળવવા અથવા અન્ય લોકોની ઓળખનો ઉપયોગ કરીને સિમકાર્ડ સક્રિય કરાવવાની પ્રક્રિયા આ ગેરકાયદે વ્યવસાયનો પાયો બને છે. આ રીતે તૈયાર થયેલા મોબાઈલ નંબર અને તેના પર આવતા વેરિફિકેશન કોડ વિદેશમાં બેઠેલા હેન્ડલર્સ સુધી પહોંચાડવામાં આવે છે.પરિણામે, વિદેશમાં બેઠેલા સાયબર ગુનેગારો ભારતીય મોબાઈલ નંબરના આધારે એકાઉન્ટ ચલાવી શકે છે, જ્યારે મૂળ સિમકાર્ડ અને તેની સાથે જોડાયેલી ઓળખ ભારતમાં જ હોય છે.



ભારતમાં સિમકાર્ડ ખરીદવામાં આવે છે. | વેરિફિકેશન OTP મેળવવા માટે તેનો ઉપયોગ થાય છે. | એકાઉન્ટ વિદેશમાં બેઠેલા હેન્ડલરોને સોંપવામાં આવે છે. | એકાઉન્ટ કંબોડિયા, લાઓસ અને મ્યાનમાર જેવા દેશોનાં સાયબર ક્રાઇમ કેન્દ્રો સુધી પહોંચાડવામાં આવે છે.

ભારતથી કંબોડિયા, લાઓસ અને મ્યાનમાર સુધી નેટવર્ક

આ સમગ્ર પ્રવૃત્તિનું સૌથી ચિંતાજનક પાસું તેનું આંતરરાષ્ટ્રીય જોડાણ છે. તપાસમાં કંબોડિયા, લાઓસ અને મ્યાનમાર જેવા દક્ષિણ-પૂર્વ એશિયાના દેશોમાં કાર્યરત સાયબર ક્રાઇમ નેટવર્ક સાથે ભારતીય મોબાઇલ નંબર અને વોટ્સએપ એકાઉન્ટની કડીઓ હોવાની વિગતો સામે આવી છે.આ દેશોમાં કેટલાક સ્થળોએ સાયબર છેતરપિંડીના સંગઠિત કેન્દ્રો કાર્યરત હોવાના અહેવાલો છે. અહીંથી ઓનલાઇન રોકાણની લાલચ, નકલી નોકરીની ઓફર, ડિજિટલ ધરપકડના નામે ધમકી, બેન્કિંગ છેતરપિંડી અને અન્ય પ્રકારના સાયબર ગુનાઓ આચરવામાં આવે છે.ભારતીય મોબાઇલ નંબરથી બનાવવામાં આવેલા એકાઉન્ટનો ઉપયોગ કરીને સ્થાનિક નાગરિકોનો વિશ્વાસ જીતવો સરળ બને છે. અજાણ્યા આંતરરાષ્ટ્રીય નંબર કરતાં ભારતીય નંબર પરથી આવતા મેસેજને લોકો વધુ વિશ્વસનીય માની લેતા હોય છે. આ માનસિકતાનો જ ગુનેગારો લાભ લેતા હોવાની આશંકા છે.

પોલીસ તપાસમાં ચોંકાવનારા કિસ્સા

દેશના વિવિધ રાજ્યોમાં થયેલી તપાસ દરમિયાન આ નેટવર્કની કામગીરી અંગે અનેક વિગતો સામે આવી છે.ઉત્તર પ્રદેશમાં વર્ષ 2020માં એક સિમકાર્ડ રિટેલરની ધરપકડ કરવામાં આવી હતી. ગ્રાહકોના બાયોમેટ્રિક ડેટાનો દુરુપયોગ કરીને વધારાના સિમકાર્ડ મેળવવામાં આવ્યા હોવાનો આરોપ હતો.મુંબઈમાં મે 2026 દરમિયાન ચાર વ્યક્તિઓની વોટ્સએપ એકાઉન્ટ ક્લોનિંગના આરોપસર ધરપકડ કરવામાં આવી હતી. પોલીસને તેમની પાસેથી મોટી સંખ્યામાં સિમકાર્ડ મળી આવ્યા હતા અને વિદેશી સાયબર ગુનેગારો સાથેની કડીઓની તપાસ કરવામાં આવી હતી.મુંબઈમાં સપ્ટેમ્બર 2026માં પણ ત્રણ વ્યક્તિઓની ધરપકડ કરવામાં આવી હતી. તપાસમાં 669 સક્રિય સિમકાર્ડ અને 100 મોબાઇલ હેન્ડસેટ મળી આવ્યા હોવાનો અહેવાલ છે. આ સિમકાર્ડ પર જનરેટ થતા વેરિફિકેશન કોડ કંબોડિયા સ્થિત હેન્ડલર્સ સુધી પહોંડવામાં આવતા હોવાની આશંકા વ્યક્ત કરવામાં આવી હતી.જોધપુરમાં 2026 દરમિયાન થયેલી તપાસમાં કંબોડિયા આધારિત સાયબર નેટવર્ક સાથે જોડાયેલા છ લોકોની ધરપકડ કરવામાં આવી હોવાની વિગતો પણ સામે આવી છે.

સિમકાર્ડથી શરૂ થાય છે ગુનાખોરીની સફર

ઓટીપી એટલે કે વન ટાઇમ પાસવર્ડ સામાન્ય રીતે ડિજિટલ વ્યવહારો અને ઓનલાઇન એકાઉન્ટની સુરક્ષા માટે ઉપયોગમાં લેવાતો એક મહત્વપૂર્ણ કોડ છે. પરંતુ આ જ સુરક્ષા વ્યવસ્થાનો દુરુપયોગ કરીને સાયબર ગુનેગારો નવો ગુનાહિત વ્યવસાય ઊભો કરી રહ્યા છે. આ પ્રવૃત્તિને 'ઓટીપી ફાર્મિંગ' તરીકે ઓળખવામાં આવે છે.આ સમગ્ર નેટવર્કમાં સૌથી પહેલાં મોટી સંખ્યામાં સિમકાર્ડ એકત્ર કરવામાં આવે છે. કેટલાક કિસ્સાઓમાં અન્ય વ્યક્તિઓના આધારકાર્ડ અને ઓળખના દસ્તાવેજોનો દુરુપયોગ કરીને સિમકાર્ડ મેળવવામાં આવતા હોવાની વિગતો સામે આવી છે. ત્યારબાદ આ સિમકાર્ડનો ઉપયોગ વોટ્સએપ સહિત વિવિધ મેસેજિંગ પ્લેટફોર્મ પર એકાઉન્ટ બનાવવામાં થાય છે.
એક જ વ્યક્તિના નામે અનેક સિમકાર્ડ મેળવવા અથવા અન્ય લોકોની ઓળખનો ઉપયોગ કરીને સિમકાર્ડ સક્રિય કરાવવાની પ્રક્રિયા આ ગેરકાયદે વ્યવસાયનો પાયો બને છે. આ રીતે તૈયાર થયેલા મોબાઇલ નંબર અને તેના પર આવતા વેરિફિકેશન કોડ વિદેશમાં બેઠેલા હેન્ડલર્સ સુધી પહોંચાડવામાં આવે છે.