TECH BITES

બ્યુટી ઈન્ડસ્ટ્રીમાં AIનું વધતું પ્રભુત્વ, હવે વધુ વ્યક્તિગત બનશે

L'Oral અને OpenAIની ભાગીદારીથી વ્યક્તિગત બ્યુટી સલાહ મળશે. કોસ્મેટિક્સ કંપની L'Oral અને OpenAI વચ્ચે થયેલી ભાગીદારી બાદ ગ્રાહકોને ChatGPT દ્વારા વ્યક્તિગત બ્યુટી સલાહ, મેકઅપ સૂચનો અને પ્રોડક્ટ ભલામણો મળી શકશે. AI આધારિત બ્યુટી અનુભવ હવે વધુ વ્યક્તિગત બનશે.

AI સંગીત ઉદ્યોગ માટે પડકાર: કલાકારો માંગે છે મંજૂરી

વિશ્વભરના સંગીતકારો અને સંગીત સંસ્થાઓએ માંગ કરી છે કે AI દ્વારા ગીતો, અવાજ અને સંગીતનો ઉપયોગ કરતા પહેલાં કલાકારોની સ્પષ્ટ મંજૂરી લેવામાં આવે. AIના વધતા ઉપયોગને કારણે કોપિરાઇટ અને બૌદ્ધિક સંપત્તિના પ્રશ્નો વધુ ગંભીર બન્યા છે. આ માટે સરકાર પણ વિચાર કરી રહી છે.

AIથી બનેલા વિડિયોનો નવો રેકોર્ડ,Closeup અભિયાન સફળ

હિંદુસ્તાન યુનિલીવરની Closeup બ્રાન્ડે AI આધારિત વ્યક્તિગત મ્યુઝિક વિડિયો અભિયાન ચલાવીને એશિયા બુક ઓફ રેકોર્ડ્સ અને ઈન્ડિયા બુક ઓફ રેકોર્ડ્સમાં સ્થાન મેળવ્યું છે. યુઝર્સ પોતાની સેલ્ફી અપલોડ કરીને AIની મદદથી વ્યક્તિગત મ્યુઝિક વિડિયો બનાવી શક્યા, જેને લાખો લોકોએ પસંદ કર્યો.

ઝડપ માટે રચાયેલી ટેક્નોલોજી કેવી રીતે વપરાશકર્તાઓને અનિચ્છિત ભૂલો તરફ ધકેલી રહી છે

એક ટૅપની કિંમત I ડિજિટલ દુનિયામાં ઉતાવળ અને પછી શરૂ પસ્તાવાનું ચક્ર

સ્માર્ટફોન, સોશિયલ મીડિયા અને ડિજિટલ પેમેન્ટના યુગમાં માનવીનું જીવન પહેલાં કરતાં વધુ સરળ અને ઝડપી બની ગયું છે. એક જ ટૅપમાં પૈસા ટ્રાન્સફર થઈ જાય છે, ખરીદી પૂર્ણ થઈ જાય છે, ફોટા અને સંદેશાઓ દુનિયાના કોઈપણ ખૂણે પહોંચાડી શકાય છે. પરંતુ આ ઝડપ અને સરળતાની પાછળ એક એવી હકીકત પણ છુપાયેલી છે, જે ધીમે ધીમે માનવીને ઉતાવળ અને પસ્તાવાના ચક્રમાં ધકેલી રહી છે. નિષ્ણાતોનું માનવું છે કે "ફ્રિક્શનલેસ ડિઝાઈન" તરીકે ઓળખાતી આ ટેક્નોલોજી વપરાશકર્તાઓને વિચારવાનો સમય આપતી નથી અને ઘણી વખત એક ક્ષણની ભૂલ લાંબા ગાળાના નુકસાનનું કારણ બની શકે છે.

સુવિધા અને સુરક્ષા વચ્ચેનું સંતુલન જાળવવાનો સમય આવી ગયો છે

ડિજિટલ સુરક્ષામાં 'વિચારનો વિરામ' જરૂરી

સાયબર સુરક્ષા નિષ્ણાતો માને છે કે દરેક પ્રક્રિયાને સંપૂર્ણપણે સરળ બનાવી દેવી યોગ્ય નથી. કેટલીક જગ્યાએ "ફ્રિક્શન" અથવા વિચારવાનો થોડોક સમય જરૂરી છે. બે-સ્ટેપ ઓથેન્ટિકેશન, ટ્રાન્ઝેક્શન પહેલાં કન્ફર્મેશન સ્ક્રીન, પાસવર્ડ ચકાસણી અને સુરક્ષા એલર્ટ જેવી વ્યવસ્થાઓ વપરાશકર્તાને ભૂલો અને છેતરપિંડીથી બચાવી શકે છે.ભારતમાં ડિજિટલ પેમેન્ટ અને ઓનલાઈન ટ્રાન્ઝેક્શનના ઝડપથી વધતા ઉપયોગ વચ્ચે સાયબર ફ્રોડના કેસોમાં પણ વધારો નોંધાઈ રહ્યો છે. તેથી માત્ર ઝડપને જ સફળતા ગણવાને બદલે સુરક્ષા અને જવાબદારીને પણ પ્રાથમિકતા આપવાની જરૂર છે. દરેક વપરાશકર્તાએ અજાણી લિંક પર ક્લિક કરતા પહેલાં તેની ચકાસણી કરવી, સત્તાવાર એપ્લિકેશનનો જ ઉપયોગ કરવો અને સમયાંતરે પાસવર્ડ બદલવાની ટેવ વિકસાવવી જોઈએ.

વધતી ડિજિટલ ભૂલો

આજના સમયમાં ખોટા વ્યક્તિને મેસેજ મોકલવો, ઉતાવળમાં સોશિયલ મીડિયા પર કંઈક પોસ્ટ કરી દેવું, ભૂલથી ઓનલાઈન સબ્સ્ક્રિપ્શન ખરીદી લેવી અથવા ખોટા ખાતામાં પૈસા ટ્રાન્સફર થઈ જવા જેવી ઘટનાઓ સામાન્ય બની ગઈ છે. ઘણા લોકો પોતાનો અનુભવ શેર કરતાં કહે છે કે એક ક્ષણની બેદરકારીના કારણે તેમને આર્થિક નુકસાન ઉપરાંત માનસિક તણાવનો પણ સામનો કરવો પડ્યો છે.ડિજિટલ પ્લેટફોર્મ્સનો મુખ્ય ઉદ્દેશ વપરાશકર્તાઓને વધુ ઝડપથી સેવા પૂરી પાડવાનો છે. તેથી ઘણી એપ્લિકેશન્સમાં પ્રક્રિયાઓ એટલી સરળ બનાવી દેવામાં આવી છે કે વપરાશકર્તાને નિર્ણય લેવા માટેનો સમય જ મળતો નથી. એક જ ક્લિકમાં ખરીદી, પેમેન્ટ અથવા પોસ્ટિંગની સુવિધા ઉપયોગી તો છે, પરંતુ તેની સાથે જોખમો પણ વધી રહ્યા છે.

મગજ કરતાં ઝડપથી ચાલે છે આંગળીઓ

માનસશાસ્ત્રીઓના મતે સતત સ્માર્ટફોનનો ઉપયોગ અને ઝડપથી સ્ક્રોલિંગ કરવાની આદતને કારણે ઘણી વખત આંગળીઓ મગજના નિર્ણય કરતાં ઝડપથી કામ કરવા લાગે છે. પરિણામે વ્યક્તિ વિચાર્યા વગર જ કોઈ ક્રિયા કરી બેસે છે. સોશિયલ મીડિયા અને ઈ-કોમર્સ કંપનીઓ વપરાશકર્તાઓને વધુ સમય સુધી જોડાયેલા રાખવા માટે એવી ડિઝાઇન અપનાવે છે, જેમાં ઓછામાં ઓછા અવરોધ હોય. આ મોડેલથી કંપનીઓને ફાયદો થાય છે, પરંતુ વપરાશકર્તાઓ માટે ભૂલોની સંભાવના વધી જાય છે.

ટેક્નોલોજીનો આગામી પડકાર I ઝડપ નહીં, સમજદારી

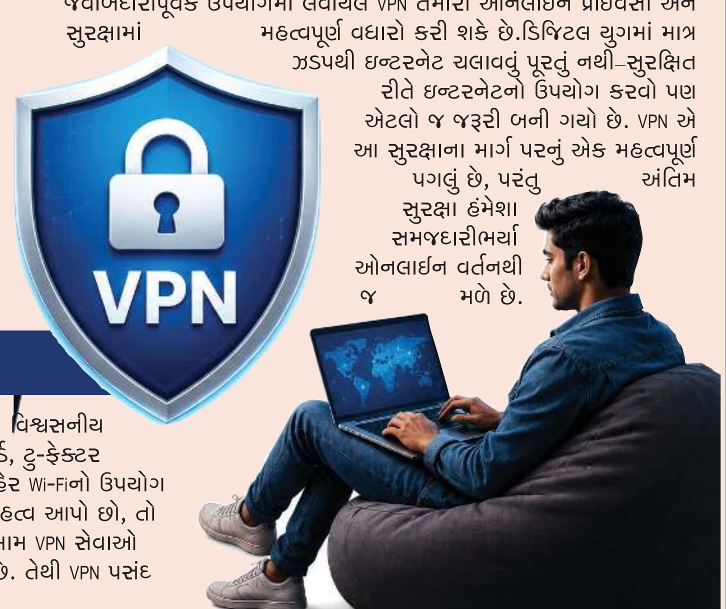
ટેક્નોલોજી ક્ષેત્રના નિષ્ણાતોનું માનવું છે કે ભવિષ્યમાં સફળ ડિજિટલ પ્લેટફોર્મ્સ માત્ર ઝડપી નહીં, પરંતુ વધુ જવાબદાર અને માનવકેન્દ્રિત બનશે. વપરાશકર્તાઓને ઉતાવળમાં નિર્ણય લેવાને બદલે થોડોક વિચારવાનો સમય આપતી સિસ્ટમો વધુ વિશ્વસનીય સાબિત થશે.આખરે, એક ટૅપ જીવનને સરળ બનાવી શકે છે, પરંતુ એ જ એક ટૅપ પસ્તાવાનું કારણ પણ બની શકે છે. તેથી ડિજિટલ યુગમાં સૌથી મોટું શસ્ત્ર માત્ર સ્માર્ટફોન નહીં, પરંતુ સાવચેતી અને સમજદારી છે. ઝડપથી ભરેલી આ દુનિયામાં ક્યારેક થોડું થોભવું જ સૌથી સમજદાર નિર્ણય બની શકે છે.

સાયબર જોખમોના યુગમાં VPNની વધતી લોકપ્રિયતા પાછળનું સત્ય

ડિજિટલ દુનિયામાં પ્રાઈવસીનું નવું હથિયાર

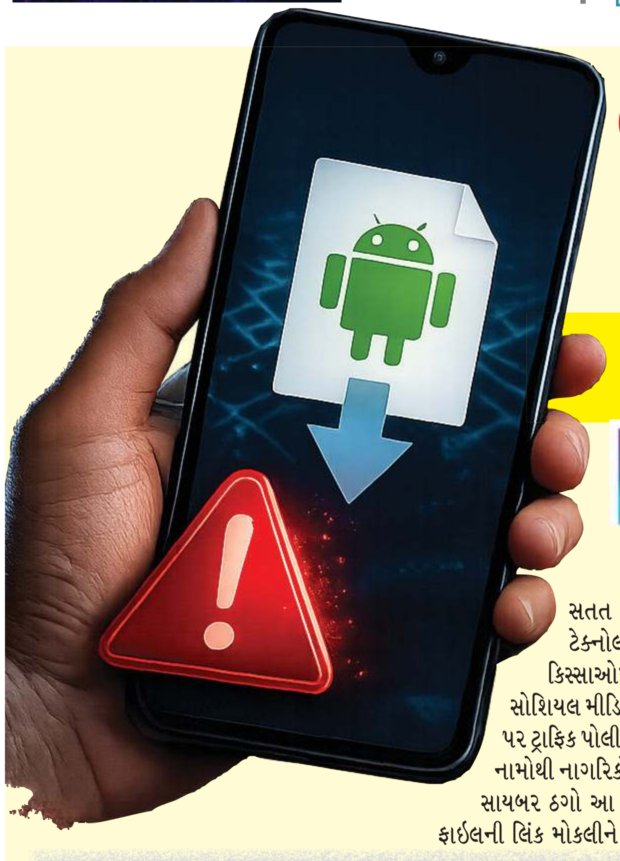
આજના ડિજિટલ યુગમાં વ્યક્તિગત માહિતી સૌથી મૂલ્યવાન સંપત્તિ બની ગઈ છે. બેન્કિંગ, સોશિયલ મીડિયા, ઓફિસનું કામ, ઓનલાઈન શોપિંગ અને સરકારી સેવાઓ–જીવનનો મોટો હિસ્સો હવે ઈન્ટરનેટ પર આધારિત છે. પરંતુ જેટલી સુવિધાઓ વધી રહી છે, એટલા જ સાયબર હુમલા, ડેટા ચોરી અને ઓનલાઈન દેખરેખના જોખમો પણ વધી રહ્યા છે. આ પરિસ્થિતિમાં Virtual Private Network (VPN) એક અસરકારક સુરક્ષા સાધન તરીકે ઉભરી આવ્યું છે. VPN તમારા ડિવાઈસ અને ઈન્ટરનેટ વચ્ચે એક સુરક્ષિત, એન્ક્રિપ્ટેડ ટનલ બનાવે છે, જેના કારણે તમારી ઓનલાઈન પ્રવૃત્તિ અન્ય લોકો માટે જોવી મુશ્કેલ બને છે. જાહેર Wi-Fiનો ઉપયોગ કરતી વખતે VPN ખાસ ઉપયોગી સાબિત થાય છે, કારણ કે તે હેકર્સ સામે વધારાનું રક્ષણ આપે છે. તાજેતરના વર્ષોમાં ભારતમાં VPNનો ઉપયોગ ઝડપથી વધ્યો છે. ખાસ કરીને ગોપનીયતા જાળવવા, ડેટા સુરક્ષિત રાખવા અને કેટલાક પ્રતિબંધિત ઓનલાઈન કન્ટેન્ટને ઍક્સેસ કરવા માટે લોકો VPN તરફ વળી રહ્યા છે. વિદ્યાર્થીઓ, પત્રકારો, વકીલો, બિઝનેસ પ્રોફેશનલ્સ અને રિમોટ વર્કર્સ માટે VPN હવે એક જરૂરી ટૂલ બની રહ્યું છે. બજારમાં ઉપલબ્ધ તમામ VPN સેવાઓ વિશ્વસનીય હોતી નથી. કેટલીક મફત VPN એપ્સ યુઝરના ડેટા એકત્રિત કરીને વેચતી હોવાના આરોપો પણ સામે આવ્યા છે.

સુરક્ષિત રીતે ઈન્ટરનેટનો ઉપયોગ કરવો I VPN કોઈ જાદુઈ ઢાલ નથી કે જે તમામ સાયબર જોખમોને દૂર કરી દે. પરંતુ યોગ્ય રીતે પસંદ કરાયેલ અને જવાબદારીપૂર્વક ઉપયોગમાં લેવાયેલ VPN તમારી ઓનલાઈન પ્રાઇવસી અને સુરક્ષામાં મહત્વપૂર્ણ વધારો કરી શકે છે.ડિજિટલ યુગમાં માત્ર ઝડપથી ઇન્ટરનેટ ચલાવવું પૂરતું નથી–સુરક્ષિત રીતે ઇન્ટરનેટનો ઉપયોગ કરવો પણ એટલો જ જરૂરી બની ગયો છે. VPN એ આ સુરક્ષાના માર્ગ પરનું એક મહત્વપૂર્ણ પગલું છે, પરંતુ અંતિમ સુરક્ષા હંમેશા સમજદારીભર્યા ઓનલાઈન વર્તનથી જ મળે છે.



બજારમાં ઉપલબ્ધ તમામ VPN સેવાઓ વિશ્વસનીય હોતી નથી

VPN અનેક ફાયદા આપે છે, પરંતુ તેનો અર્થ એ નથી કે દરેક ઇન્ટરનેટ યુઝર માટે તે ફરજિયાત છે. જો તમે સામાન્ય રીતે વિશ્વસનીય નેટવર્ક પર સોશિયલ મીડિયા, મનોરંજન અથવા રોજિંદા બ્રાઉઝિંગ માટે ઇન્ટરનેટનો ઉપયોગ કરો છો, તો મજબૂત પાસવર્ડ, ટુ-ફેક્ટર ઓથેન્ટિકેશન અને નિયમિત સોફ્ટવેર અપડેટ્સ ઘણી વખત પૂરતી સુરક્ષા આપી શકે છે.બીજી તરફ, જો તમે વારંવાર જાહેર Wi-Fiનો ઉપયોગ કરો છો, સંવેદનશીલ દસ્તાવેજો સાથે કામ કરો છો, આંતરરાષ્ટ્રીય મુસાફરી કરો છો અથવા ઓનલાઈન પ્રાઇવસીને વધુ મહત્વ આપો છો, તો વિશ્વસનીય VPN સેવા તમારા માટે ઉપયોગી બની શકે છે.પરંતુ અહીં એક મહત્વની ચેતવણી પણ છે. બજારમાં ઉપલબ્ધ તમામ VPN સેવાઓ વિશ્વસનીય હોતી નથી. કેટલીક મફત VPN એપ્સ યુઝરના ડેટા એકત્રિત કરીને વેચતી હોવાના આરોપો પણ સામે આવ્યા છે. તેથી VPN પસંદ કરતી વખતે તેની પ્રાઇવસી પોલિસી, સર્વર નેટવર્ક, સુરક્ષા સુવિધાઓ અને કંપનીની વિશ્વસનીયતા ચકાસવી જરૂરી છે.



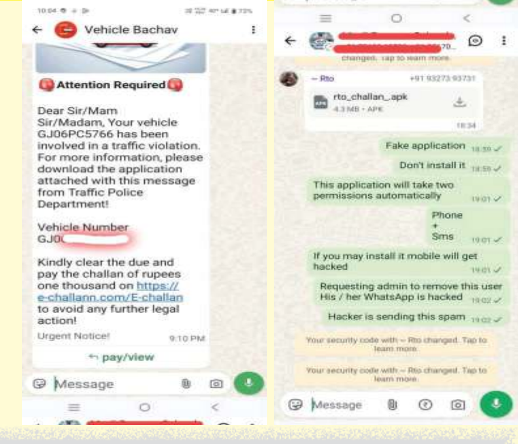
વાહન બચાવ, ઈ-ચલણ

APK ફાઈલના નામે થતી છેતરપિંડી

કોઈપણ એપ્લિકેશન હંમેશા માત્ર સત્તાવાર "Google Play Store" કે "Apple App Store" પરથી જ ડાઉનલોડ કરો

મયુર ભુસાવળકર
આઈટી એક્સપર્ટ

આજના ડિજિટલ યુગમાં સાયબર ગુનેગારો લોકોને છેતરવા માટે સતત નવા-નવા રસ્તાઓ અપનાવી રહ્યા છે. ટેક્નોલોજીના વધતા ઉપયોગ સાથે છેતરપિંડીના કિસ્સાઓમાં પણ નોંધપાત્ર વધારો થયો છે. હાલમાં સોશિયલ મીડિયા, વોટ્સએપ અને અન્ય મેસેજિંગ પ્લેટફોર્મ પર ટ્રાફિક પોલીસ અથવા "Vehicle Bachav" જેવા નકલી નામોથી નાગરિકોને છેતરવાના બનાવો ઝડપથી વધી રહ્યા છે. સાયબર ઠગો આ પ્રકારની નકલી એપ્લિકેશન અથવા APK ફાઈલની લિંક મોકલીને ઠગાઈ કરતાં હોય છે.



સાયબર ફ્રોડથી બચવા માટે શું કરવું?

કોઈપણ લિંક પર ક્લિક ન કરો: વોટ્સએપ કે એસએમએસ પર આવેલી અજાણી લિંક્સ પર ક્લિક કરવાનું ટાળો. સત્તાવાર સરકારી ઇ-ચલાણની વેબસાઇટ હંમેશા .gov.in (જેમ કે echallan.parivahan.gov.in) ડોમેન ધરાવતી હોય છે.

અજાણી APK ફાઈલ ક્યારેય ઈન્સ્ટોલ ન કરો: વોટ્સએપ પરથી ડાઉનલોડ થયેલી કોઈપણ .apk ફાઇલ ફોનમાં રન કે ઇન્સ્ટોલ કરશો નહીં. કોઈપણ એપ્લિકેશન હંમેશા માત્ર સત્તાવાર "Google Play Store" કે "Apple App Store" પરથી જ ડાઉનલોડ કરો.

પરવાનગીઓ તપાસો: જો કોઈ એપ ભૂલથી ડાઉનલોડ થઈ જાય, તો તેને SMS કે ફોન કોલ્સની પરવાનગી બિલકુલ ન આપો.

અન્ય લોકોને જાગૃત કરો: જો તમારા કોઈ ગ્રૂપમાં આવી શંકાસ્પદ ફાઇલ આવે, તો ગ્રૂપ એડમિનને કહીને તે યુઝરને તરત જ રીમૂવ કરો અથવા બ્લોક કરો, કારણ કે તેનું એકાઉન્ટ હેક થયેલું હોઈ શકે છે.

ફરિયાદ દાખલ કરવા માટે: જો તમે આવા કોઈ સાયબર ફ્રોડનો ભોગ બનો છો, તો વિલંબ કર્યા વિના તરત જ રાષ્ટ્રીય સાયબર હેલ્પલાઇન નંબર 1930 પર કોલ કરો અથવા સત્તાવાર સાયબર ક્રાઇમ પોર્ટલ www.cybercrime.gov.in પર તમારી ફરિયાદ નોંધાવો.

બે મુખ્ય પદ્ધતિ દ્વારા લોકોને શિકાર બનાવે છે

1) નકલી ઈ-ચલાણની લિંક અને મેસેજ : આ પ્રકારના ફ્રોડમાં ગુનેગારો તમારા વાહનનો સાચો કે ખોટો નંબર મેળવીને તમને ડરાવવા માટે એક તાકીદનો મેસેજ મોકલે છે. જેમ કે: "તમારા વાહને ટ્રાફિક નિયમોનું ઉલ્લંઘન કર્યું છે અને કાનૂની કાર્યવાહીથી બચવા માટે તરત જ આપેલ લિંક પર ક્લિક કરીને ૧૦૦૦નું ચલાણ ભરો."
જોખમ: આ મેસેજમાં આપેલી લિંક (દા.ત. e-challann.com) નકલી હોય છે. તમે ક્લિક કરશો, તે તમને સરકારી વેબસાઇટ જેવી જ દેખાતી નકલી વેબસાઇટ પર લઈ જશે અને તમારી બેંકિંગ વિગતો અથવા યુપીઆઈ પિન ચોરી લેશે.

2) નકલી એપ્લિકેશન (.APK ફાઈલ) મોકલવી:મેસેજની સાથે ગુનેગારો rto_challan_.apk જેવી એન્ડ્રોઇડ એપ્લિ. ફાઇલ સીધી વોટ્સએપ ગ્રૂપ કે પર્સનલ ચેટમાં મોકલે છે. ચલાણની વિગતો માટે તેને ઇન્સ્ટોલ કરવા કહે છે.
જોખમ: આ કોઈ સત્તાવાર એપ નથી હોતી પરંતુ એક ઘાતક વાયરસ હોય છે. એકવાર તમે આ એપ્લિકેશન ફોનમાં ઇન્સ્ટોલ કરો, એટલે તે તમારા ફોનના SMS અને કોલ ની પરવાનગીઓ આપમેળે લઈ લે છે. આનાથી હેકર્સ તમારા બેંકના OTP વાંચી શકે છે અને તમારો ફોન કે સોશિયલ મીડિયા એકાઉન્ટ સંપૂર્ણપણે હેક થઈ શકે છે.

શું ગ્રાહકો પાસે ખરેખર વિકલ્પો બચ્યા છે?

ડિજિટલ દુનિયા પર બિગ ટેકનો દબદબો

ડિજિટલ યુગમાં ગ્રાહકો ખરેખર પસંદગીની સ્વતંત્રતા ધરાવે છે કે પછી તેઓ અજાણતાં જ બિગ ટેકના ઈકોસિસ્ટમમાં બંધાઈ ગયા છે?

આજના ડિજિટલ યુગમાં ટેક્નોલોજીએ જીવનને સરળ બનાવ્યું છે, પરંતુ તેની સાથે એક નવી ચિંતા પણ ઉભી થઈ રહી છે. સર્ચ એન્જિન, ઈ-મેઈલ, મેપ્સ, વીડિયો કોલ અને સોશિયલ મીડિયા જેવી રોજિંદી સેવાઓ પર અમુક મોટી ટેક્નોલોજી કંપનીઓનું પ્રભુત્વ એટલું વધી ગયું છે કે ગ્રાહકો માટે અન્ય વિકલ્પો અપનાવવાનું મુશ્કેલ બનતું જઈ રહ્યું છે. ભારતમાં 500 શહેરી ગ્રાહકો પર કરાયેલા સર્વેમાં જાણવા મળ્યું કે મોટા ભાગના લોકો ગૂગલની વિવિધ સેવાઓ પર ખૂબ જ નિર્ભર છે. લગભગ તમામ પ્રતિભાગીઓ સર્ચ અને ઈ-મેઈલ માટે ગૂગલનો ઉપયોગ કરે છે, જ્યારે 98 ટકા લોકો ક્રોમ, 97 ટકા લોકો ગૂગલ મેપ્સ અને 96 ટકા લોકો ગૂગલ ડ્રાઈવનો ઉપયોગ કરે છે. વીડિયો કમ્યુનિકેશન માટે પણ વોટ્સએપ અને ગૂગલ મીટનું પ્રભુત્વ જોવા મળે છે. સર્વેમાં સામે આવ્યું કે અડધાથી વધુ લોકોને એક પ્લેટફોર્મમાંથી બીજા પ્લેટફોર્મમાં ડેટા ટ્રાન્સફર કરવામાં મુશ્કેલી પડે છે. 48 ટકા લોકોએ જણાવ્યું કે તેમના મિત્રો અને સંપર્કો અન્ય પ્લેટફોર્મ પર હોવાથી તેઓ સેવા બદલવા ઈચ્છતા નથી, જ્યારે 35 ટકા લોકોને ભય છે કે પ્લેટફોર્મ બદલવાથી અગાઉની ખરીદીઓ અથવા સબ્સ્ક્રિપ્શન ગુમાવવાનો વારો આવી શકે છે. નિષ્ણાતોના મતે, આ પરિસ્થિતિ માત્ર ગ્રાહકો માટે જ નહીં, પરંતુ નવી ટેક્નોલોજી કંપનીઓ અને સ્ટાર્ટઅપ્સ માટે પણ પડકારરૂપ છે.

મોટા પ્લેટફોર્મ્સની મજબૂત ઈકોસિસ્ટમ અને વિશાળ વપરાશકર્તા આધારને કારણે નવા ખેલાડીઓને બજારમાં સ્થાન મેળવવું મુશ્કેલ બની રહ્યું છે. આર્ટિફિશિયલ ઈન્ટેલિજન્સ (AI)ના વધતા ઉપયોગ સાથે આ પ્રભુત્વ વધુ મજબૂત બનવાની આશંકા વ્યક્ત કરવામાં આવી રહી છે. પ્રી-ઈન્સ્ટોલ્ડ AI સહાયકો અને સંકલિત સેવાઓ ગ્રાહકોને ચોક્કસ ઈકોસિસ્ટમ સાથે વધુ જોડાયેલા રાખી શકે છે. વિશ્લેષકોનું માનવું છે કે ગ્રાહકોને વધુ વિકલ્પો, સરળ ડેટા પોર્ટેબિલિટી અને પારદર્શક ડિજિટલ બજાર ઉપલબ્ધ કરાવવું સમયની માંગ બની ગયું છે. કારણ કે ડિજિટલ અર્થવ્યવસ્થામાં સ્પર્ધા જેટલી મજબૂત હશે, નવીનતા અને ગ્રાહકોના હિતો એટલા જ વધુ સુરક્ષિત રહેશે. આખરે પ્રશ્ન એ જ છે કે ડિજિટલ યુગમાં ગ્રાહકો ખરેખર પસંદગીની સ્વતંત્રતા ધરાવે છે કે પછી તેઓ અજાણતાં જ બિગ ટેકના ઈકોસિસ્ટમમાં બંધાઈ ગયા છે?