

TECH BITES

AI આધારિત ડાયાબિટિક રેટિનોપેથી સ્ક્રીનિંગથી ખર્ચમાં ઘટાડો



ડાયાબિટીસના દર્દીઓમાં આંખની રેટિનાને નુકસાન થતું અટકાવવા માટે નિયમિત સ્ક્રીનિંગ મહત્વપૂર્ણ છે. Ophthalmology Retinaમાં પ્રકાશિત અભ્યાસ અનુસાર, AI આધારિત ડાયાબિટિક રેટિનોપેથી સ્ક્રીનિંગથી નિદાનની અસરકારકતા વધારવાની સાથે સારવાર સુધી પહોંચ સુધારી શકાય છે. પરંપરાગત સ્ક્રીનિંગની સરખામણીએ AI આધારિત પદ્ધતિમાં દર્દી દીઠ ખર્ચમાં પણ નોંધપાત્ર ઘટાડો જોવા મળ્યો હતો. અભ્યાસ મુજબ, AI આધારિત સ્ક્રીનિંગનો પ્રતિ દર્દી ખર્ચ આશરે 27.35 ડોલર રહ્યો હતો, જ્યારે નિયમિત સ્ક્રીનિંગનો ખર્ચ 43.14 ડોલર હતો. આ ટેકનોલોજી ખાસ કરીને મોટી સંખ્યામાં દર્દીઓનું ઝડપી અને અસરકારક સ્ક્રીનિંગ કરવામાં ઉપયોગી સાબિત થઈ શકે છે.

એફકોમ બોઈંગ પાસેથી ચાર 777-8F ફેઈટર એરક્રાફ્ટ ખરીદશે



એફકોમ હોલ્ડિંગ્સ લિમિટેડે ચાર બોઈંગ 777-8F ફેઈટર એરક્રાફ્ટ ખરીદવા માટે બોઈંગ કંપની સાથે લેટર ઓફ ઇન્ટેન્ડ (LOI) પર હસ્તાક્ષર કર્યા છે. આ પ્રસ્તાવિત ખરીદી કંપનીના કાફલા વિસ્તરણ અને આંતરરાષ્ટ્રીય વિકાસ માટે મહત્વપૂર્ણ પગલું છે. 777-8F ફેઈટર એફકોમના હાલના B737-800 ફેઈટર્સની તુલનામાં લગભગ પાંચ ગણી કાર્ગો ક્ષમતા ધરાવે છે અને 10થી 12 કલાક કે તેથી વધુ સમયના લાંબા રૂટ માટે ઉપયોગી બનશે. નવા વિમાનો દ્વારા કંપની લાંબા અંતરના એર કાર્ગો ઓપરેશન, આંતરરાષ્ટ્રીય જોડાણ અને મુખ્ય વેપાર કોરિડોરમાં પોતાની હાજરી મજબૂત કરવાની દિશામાં આગળ વધશે.

AI એજન્ડ્સ દ્વારા જર્મન વેબસાઈટ DseWiki હાઈજેક



AI એજન્ડ્સની વધતી ક્ષમતાઓ સાથે તેમની સુરક્ષા અંગેના સવાલો પણ ગંભીર બની રહ્યા છે. Nightingale Collectiveના એક અહેવાલમાં દાવો કરવામાં આવ્યો છે કે OpenAIના AI એજન્ડ્સે જર્મન વેબસાઇટ DseWikiને હાઇજેક કરી હતી. અહેવાલ અનુસાર, આ ઘટના કંપની દ્વારા Hugging Face પર થયેલા હુમલાની માહિતી જાહેર કરવામાં આવી તેના કેટલાક મહિના પહેલાં બની હતી. AI એજન્ડ્સે કથિત રીતે વેબસાઇટનો ઉપયોગ પોતાના સંદેશા બોર્ડ તરીકે કર્યો હતો. આ ઘટનાએ AI એજન્ડ્સને મળતી સ્વાયત્તતા, વેબસાઇટ્સ પર તેમના નિયંત્રણ અને ડિજિટલ સિસ્ટમની સુરક્ષા અંગે ચિંતા વધારી છે. આના વધતા ઉપયોગ વચ્ચે આવા બનાવો સામે મજબૂત સુરક્ષા વ્યવસ્થા જરૂરી બની રહી છે.

ચુસ્ત કંટ્રોલમાંથી બહાર નીકળતા AIના કેસોમાં તીવ્ર વધારો



AI સિસ્ટમ્સને લઈને સૌથી મોટી ચિંતાઓમાંની એક તેમનું માનવ નિયંત્રણમાંથી બહાર જવું છે. તાજેતરના એક સંશોધન મુજબ, AI સિસ્ટમ્સ દ્વારા ખોટું બોલવું, સૂચનાઓની અવગણના કરવી અને પોતાના લક્ષ્યો હાંસલ કરવા માટે હાનિકારક રીતો અપનાવવાના બનાવોમાં નોંધપાત્ર વધારો થયો છે. અહેવાલ અનુસાર, જૂલાઈ દરમિયાન આવા AI ‘લોસ-ઓફ-કંટ્રોલ’ બનાવો લગભગ બમણા થઈ ગયા હતા અને 300થી વધુ કેસ નોંધાયા હતા. આ સ્થિતિ AI એજન્ડ્સની વધતી સ્વાયત્તતા અંગે ગંભીર પ્રશ્નો ઉભા કરે છે. ભવિષ્યમાં AIનો વ્યાપ વધે તેમ તેની કામગીરી પર માનવીય દેખરેખ, નિયંત્રણ અને સલામતીના નિયમો વધુ મજબૂત બનાવવાની જરૂરિયાત વધી શકે છે.

ઓનલાઈન શોપિંગના 5 નિયમ

- માત્ર અધિકૃત એપ અથવા વેબસાઈટ પરથી ખરીદી કરો.
- અખાણી વેબસાઈટની સંપૂર્ણ ચકાસણી કર્યા બાદ જ પેમેન્ટ કરો.
- તમામ મહત્વપૂર્ણ એકાઉન્ટમાં 2FA સક્રિય રાખો.
- જાહેર Wi-Fi પર બેંકિંગ કે ઓનલાઈન ટ્રાન્ઝેક્શન ટાળો.
- નવી કે શંકાસ્પદ વેબસાઈટ સાથે કાર્ડ-બેંકિંગ વિગતો શેર ન કરો.

સત્તાવાર એપ અથવા વેબસાઈટ પર જઈને પ્રોડક્ટ શોધવી વધુ સલામત



હવે એઆઈ લેંગ્વેજ ટૂલ્સ દ્વારા અત્યંત શુદ્ધ અને વિશ્વાસપાત્ર ભાષામાં વ્યક્તિગત મેસેજ તૈયાર કરવામાં આવે છે. “તમારો ઓર્ડર અટકી ગયો છે” અથવા “માત્ર પાંચ રૂપિયા ચૂકવીને સરનામું અપડેટ કરો” જેવા મેસેજ દ્વારા ગ્રાહકોને નકલી લિંક પર લઈ જઈ તેમની બેંકિંગ વિગતો મેળવવામાં આવે છે.સોશિયલ મીડિયા પર આકર્ષક ફ્લેશ સેલ અને નકલી રિવ્યુ પણ સાયબર ઠગોની સામાન્ય સુક્તિ બની છે. એઆઈ બોટ્સ દ્વારા કોઈ પ્રોડક્ટ માટે મોટી સંખ્યામાં નકલી સકારાત્મક રિવ્યુ અને રેટિંગ ઊભાં કરવામાં આવે છે. પરિણામે ગ્રાહક પ્રોડક્ટ અને વેચનાર બંનેને વિશ્વસનીય માની લે છે.ઓનલાઈન શોપિંગ કરતી વખતે કોઈ પણ ઓફર અસામાન્ય રીતે સસ્તી લાગે તો તેની સત્યતા તપાસવી જરૂરી છે. મોંઘી બ્રાન્ડ્સ વસ્તુ માત્ર થોડાક સો રૂપિયામાં મળતી હોવાનો દાવો ઘણી વખત છેતરપિંડીનો સંકેત હોઈ શકે છે.

ચકાસણી વિના ચૂકવણી જોખમી

વેબસાઈટના ડોમેન નામ, કંપનીની સંપર્ક વિગતો અને અન્ય માહિતીની ચકાસણી કર્યા વિના ચૂકવણી કરવી જોખમી બની શકે છે. તાકીદ ઊભી કરતી જાહેરાતો પ્રત્યે પણ ખાસ સાવચેતી રાખવી જોઈએ. “માત્ર બે મિનિટ બાકી”, “છેલ્લા ત્રણ પીસ ઉપલબ્ધ” અથવા “આ ઓફર આજે જ” જેવા સંદેશાઓ દ્વારા ગ્રાહકને વિચારવાનો સમય ન મળે તેવો પ્રયાસ કરવામાં આવે છે. ઉતાવળમાં લેવાયેલો નિર્ણય સાયબર છેતરપિંડી તરફ દોરી શકે છે.ઓનલાઈન ખરીદી માટે શક્ય હોય ત્યાં સુધી અધિકૃત એલિકેશન અથવા સત્તાવાર વેબસાઈટનો જ ઉપયોગ કરવો જોઈએ.

1930 સાયબર ફ્રોડ હેપ્લાઈન

શંકા હોય તો ખરીદી ટાળો



હિમાલયમાં પૂરનું રહસ્ય : AI સર્વરો કે ફુદરતનો કહેર? નેપાળ હોનારત માટે કેટલું જવાબદાર ‘અંડરગ્રાઉન્ડ AI સર્પર ફાર્મ’



AIનો વધતો ઉપયોગ અને હિમાલય પર દબાણ

AI સમસ્યા છે કે ઉકેલનો ભાગ?

AI અને પર્યાવરણ વચ્ચેનો સંબંધ એકતરફી નથી. એક તરફ મોટા ડેટા સેન્ટરો ઊર્જાનો વિશાળ વપરાશ કરે છે અને જો આ વીજળી ફોસિલ ફ્યુઅલમાંથી આવે તો ગ્રીનહાઉસ ગેસના ઉત્સર્જનમાં વધારો થઈ શકે છે. આ ઉત્સર્જન વૈશ્વિક તાપમાન વધારવામાં ફાળો આપે છે અને તેની અસર હિમાલય જેવા સંવેદનશીલ પ્રદેશો પર પણ પડી શકે છે.બીજી તરફ AI આધારિત મોનિટરિંગ સિસ્ટમો હિમનદીઓ, નદીઓ અને હવામાનની સ્થિતિ પર નજર રાખવામાં મદદરૂપ બની શકે છે. પૂર અથવા હિમનદી તૂટવાની સંભાવના અંગે વહેલી ચેતવણી મળે તો જાનમાલનું નુકસાન ઘટાડવામાં મદદ મળી શકે છે.આથી મૂળ પ્રશ્ન એ નથી કે ‘AI સારું કે ખરાબ?’ પરંતુ એ છે કે AIનું વિશાળ ઇન્ફ્રાસ્ટ્રક્ચર કેટલી જવાબદારીપૂર્વક ઊભું કરવામાં આવે છે. ઉપલબ્ધ માહિતીના આધારે આ દાવાને સમર્થન આપતો સૌંદર્ય વૈજ્ઞાનિક પુરાવો રજૂ થયો નથી.વૈજ્ઞાનિક દૃષ્ટિકોણ: પૂર પાછળના કારણોમાં હિમનદી તૂટવી, અતિભારે વરસાદ, ભૂસ્ખલન અને લાંબા ગાળાના હવામાન પરિવર્તન જેવા પરિબળોની તપાસ જરૂરી છે.

AI માટે પાણી કેમ મહત્વનું?

એક મહત્વનો પાઠ

ડેટા સેન્ટરના સર્વરો ભારે ગરમી પેદા કરે છે. આ ગરમી દૂર કરવા માટે વિવિધ પ્રકારની કૂલિંગ સિસ્ટમનો ઉપયોગ થાય છે. કેટલીક સિસ્ટમમાં પાણીનો પણ નોંધપાત્ર ઉપયોગ થાય છે. એટલે AIનો વ્યાપ વધે તેમ ડેટા સેન્ટરની પાણી અને ઊર્જાની જરૂરિયાત પણ પર્યાવરણ માટે મહત્વનો મુદ્દો બની શકે છે.

નેપાળની આકૃત આપણને એક મહત્વનો પાઠ આપે છે-ટેકનોલોજી જેટલી ઝડપથી વધે છે, તેટલી જ ઝડપથી તેના પર્યાવરણીય ખર્ચની ગણતરીની જરૂર છે.

બે વાસ્તવિક પરિસ્થિતિ જેવા કિસ્સા

કિસ્સો-1 : સસ્તા બ્રાન્ડેડ બૂટનો લોભ એક ગ્રાહકે સોશિયલ મીડિયા પર 8,000ના બ્રાન્ડેડ બૂટ માત્ર 799માં મળવાની જાહેરાત જોઈ. લિંક પર ક્લિક કરીને UPI મારફતે રકમ ચૂકવ્યા બાદ લાંબા સમય સુધી સામાન મળ્યો નહીં અને ફુલિકેટ વેબસાઈટનો સંપર્ક નંબર પણ બંધ થઈ ગયો.અને ગ્રાહક છેતરાયો હતો

કિસ્સો-2 : એઆઈ વીડિયો જોઈને દવાનો ઓર્ડર એક મહિલાએ એઆઈથી બનાવાયેલા વીડિયો પર વિશ્વાસ કરીને એક પ્રોડક્ટનો ઓર્ડર આપ્યો. પેમેન્ટ દરમિયાન આપવામાં આવેલી કાર્ડ વિગતોનો દુરુપયોગ થતાં તેમના ખાતામાંથી વધારાની રકમ ઉપાડી લેવામાં આવી.

સમજદારીથી ઉપયોગ કરાય તો ગુનેગારોની જાળમાં ફસાતાં બચાવી શકે છે

ટુ-ફેક્ટર ઓથેન્ટિકેશન પણ મહત્વપૂર્ણ

અખાણી વેબસાઈટ પરથી ખરીદી કરતી વખતે ચુકવણીની પદ્ધતિ અંગે પણ સાવચેતી જરૂરી છે. શક્ય હોય ત્યાં સુધી વિશ્વસનીય અને સુરક્ષિત પેમેન્ટ વિકલ્પ પસંદ કરવો જોઈએ. એકાઉન્ટ અને કાર્ડની સુરક્ષા માટે ટુ-ફેક્ટર ઓથેન્ટિકેશન સક્રિય રાખવું પણ મહત્વપૂર્ણ છે. જાહેર Wi-Fi નેટવર્ક પર બેંકિંગ કે ઓનલાઈન પેમેન્ટ ટ્રાન્ઝેક્શન કરવાનું ટાળવું જોઈએ.જો કોઈ વ્યક્તિ સાયબર છેતરપિંડીનો ભોગ બને તો ગમતરવાને બદલે તાત્કાલિક પગલાં લેવાં જરૂરી છે. બેંક અથવા કાર્ડ પ્રોવાઈડરને જાણ કરીને સંબંધિત ખાતું કે કાર્ડ સુરક્ષિત કરાવવું જોઈએ. ભારત સરકારની પર તાત્કાલિક સંપર્ક કરવો જોઈએ તેમજ જરૂરી પુરાવા સાથે સત્તાવાર સાયબર ક્રાઈમ પોર્ટલ પર રિપોર્ટ નોંધાવવી જોઈએ.આર્ટિફિશિયલ ઇન્ટેલિજન્સના ચુગમાં ડિજિટલ સુવિધાઓ સાથે જોખમો પણ વધી રહ્યા છે.