ખિસ્સામાં બોમ્બ સમાન APK !

તમારા સ્માર્ટફોનમાં છુપાયેલી ‘મલિન એપ’ જેના ખતરનાક ખેલ

APK ફાઇલ શું છે?

APK એટલે “Android Package Kit”. એન્ડ્રોઇડ ફોનમાં કોઈપણ એપ ઇન્સ્ટોલ કરવા માટે APK ફાઇલનો ઉપયોગ થાય છે. સામાન્ય રીતે જ્યારે આપણે Google Play Store પરથી એપ ડાઉનલોડ કરીએ છીએ, ત્યારે તે સુરક્ષા ચકાસણીમાંથી પસાર થયેલી હોય છે. પરંતુ સમસ્યા ત્યારે શરૂ થાય છે જ્યારે લોકો થર્ડ પાર્ટી વેબસાઇટ, વોટ્સએપ, ટેલિગ્રામ કે SMS લિંક પરથી APK ફાઇલ ડાઉનલોડ કરે છે.સાયબર ગુનેગારો લોકપ્રિય એપ્સના નામે વાયરસ ભરેલી APK ફાઇલ તૈયાર કરે છે. બહારથી તે અસલી એપ જેવી જ દેખાય છે, પરંતુ અંદરથી તે તમારા ફોન માટે ડિજિટલ ઝેર સમાન હોય છે.

મયુર ભુસાવળકર
આઈટી એક્સપર્ટ

આ જના ડિજિટલ યુગમાં સ્માર્ટફોન માત્ર વાતચીતનું સાધન નથી રહ્યું, પરંતુ વ્યક્તિગત જીવનથી લઈને બેંકિંગ, ઓફિસના ગુપ્ત દસ્તાવેજો, ફોટા, સોશિયલ મીડિયા અને નાણાકીય વ્યવહારો સુધીનું આખું વિશ્વ હવે મોબાઈલની નાની સ્ક્રીનમાં સમાઈ ગયું છે. પરંતુ જેટલી ઝડપથી ટેક્નોલોજી આગળવધી રહી છે, એટલી જ ઝડપથી સાયબર ગુનેગારો પણ નવા નવા કૌભાંડો દ્વારા લોકોના સ્માર્ટફોનને નિશાન બનાવી રહ્યા છે.તાજેતરના સમયમાં “APK ફાઇલ”ના નામે ફેલાતો સાયબર ફ્રોડ સૌથી મોટો ખતરો બની રહ્યો છે. એક ખોટી લિંક પર ક્લિક કરવું અથવા અજાણી એપ ઈન્સ્ટોલ કરવી, અને સેકન્ડોમાં આખું બેંક ખાતું સાફ થઈ શકે છે. ઘણી વખત લોકો અજાણતાં જ પોતાનો મોબાઈલ હેકર્સના હાથમાં સોંપી દે છે.

આ ફ્રોડથી તમે કેવી રીતે સુરક્ષિત રહેશો?

- માત્ર સત્તાવાર એપ સ્ટોરનો ઉપયોગ કરો
- Google Play Store અથવા Apple App Store સિવાયથી એપ ક્યારેય ડાઉનલોડ ન કરો.
- Unknown Sources OFF રાખો
- ફોનના સેટિંગ્સમાં “Install Unknown Apps” વિકલ્પ હંમેશા બંધ રાખો.
- Play Protect ચાલુ રાખો
- Google Play Protect નુકસાનકારક એપ્સને શોધવામાં મદદ કરે છે.
- પરવાનગીઓ વાંચ્યા વગર Allow ન કરો
- ટોર્ચ એપ SMS વાંચવાની પરવાનગી માંગે તો સમજી જવું જોઈએ કે કંઈક ગડબડ છે.
- ફોન અપડેટ રાખો
- નવી સુરક્ષા અપડેટ્સ ફોનને હેકર્સથી બચાવે છે.
- જો APK આપોઆપ ડાઉનલોડ થઈ જાય તો?
- તરત “Install” પર ક્લિક ન કરો
- Downloads ફોલ્ડરમાં જઈ APK ફાઇલ Permanently Delete કરો
- બ્રાઉઝર Cache Clear કરો

સાયબર ફ્રોડ: આજનો સૌથી મોટો ખતરો

સાયબર ફ્રોડ વિશ્વનો સૌથી ઝડપથી વધતો અને સૌથી મોટો ખતરો બની ગયો છે. ભારતમાં દર વર્ષે લાખો લોકો આનો ભોગ બને છે અને કરોડો રૂપિયાનું નુકસાન થાય છે. ફેક વેબસાઇટ, ફિશિંગ લિંક, ફેક કોલ, OTP સ્કેમ અને UPI ફ્રોડ દ્વારા અપરાધીઓ સરળતાથી લોકોના બેંક ખાતા ખાલી કરી દે છે.આ ફ્રોડ માત્ર આર્થિક નુકસાન જ નથી કરતું, પરંતુ વ્યક્તિની માનસિક શાંતિ, ક્રેડિટ સ્કોર અને ડિજિટલ સુરક્ષા પણ નષ્ટ કરે છે.

1930 પર તરત કોલ કરો અને cybercrime.gov.in પર ફરિયાદ કરો. સાવધાની જ સૌથી મોટી સુરક્ષા છે

તાત્કાલિક મદદ ક્યાં મળશે?

જો કોઈ સાયબર ફ્રોડનો ભોગ બને અને બેંકિંગ નુકસાન થાય તો ગોલ્ડન અવર દરમિયાન તરત જ 1930 પર કોલ કરો અથવા ભારત સરકારના સત્તાવાર પોર્ટલ cybercrime.gov.in પર ફરિયાદ નોંધાવો. તરત જ કાર્યવાહી કરવાથી તમારા પૈસા પાછા મેળવવાની તક વધે છે. ફરિયાદમાં વિગતવાર માહિતી જેમ કે ટ્રાન્ઝેક્શન ID, તારીખ, સમય, ફ્રોડ વેબસાઇટ/એપ, સ્ક્રીનશોટ અને તમારા બેંક એકાઉન્ટની વિગતો આપો. બેંકને પણ તુરંત જાણ કરો અને ટ્રાન્ઝેક્શન બ્લોક કરાવો.

લોકો કેવી રીતે ફસાય છે?

સાયબર ઠગો સીધું “વાયરસ” લખીને કંઈ મોકલતા નથી. તેઓ ડર, ઉત્સુકતા અને લાલચનો ઉપયોગ કરે છે.

RTO ચલાન સ્કેમ
“તમારી ગાડીનું 2500નું ચલાન બાકી છે” એવો મેસેજ મોકલી લિંક અપાય છે. લિંક ખોલતા જ APK ફાઇલ ડાઉનલોડ થઈ જાય છે.

લગ્ન કંકોતરી સ્કેમ
“લગ્નની ડિજિટલ કંકોતરી” નામે APK મોકલવામાં આવે છે. લોકો PDF સમજીને ક્લિક કરે છે અને ફોનમાં વાયરસ ઘૂસી જાય છે.

સરકારી યોજના સ્કેમ
“સરકાર 5000 સહાય આપી રહી છે” અથવા “મફત સોલાર યોજના” જેવી લાલચ આપતી લિંક મોકલી લોકોને નકલી એપ ઇન્સ્ટોલ કરાવવામાં આવે છે.

એકવાર ઈન્સ્ટોલ થયા પછી શું થાય?

એકવાર APK ઇન્સ્ટોલ થઈ જાય પછી સાયબર હુમલો શરૂ થાય છે.
ફોનના SMS વાંચવાની પરવાનગી માંગે છે
બેંક OTP ચોરી લે છે
ગેલેરી, કોન્ટેક્ટ અને ચેટ્સ સર્વર પર મોકલે છે
કેમેરા અને માઇક્રોફોન દ્વારા જાસૂસી કરે છે
બેંકિંગ એપ ઉપર નકલી સ્ક્રીન બતાવી પાસવર્ડ ચોરી લે છે
ઘણા કેસોમાં તો એપ પોતાનું નામ બદલી “System Update” અથવા “Google Service” બની જાય છે જેથી યુઝરને શંકા પણ ન જાય.

સૌથી મોટું નુકસાન કયુ છે? 1. બેંક ખાતામાંથી નાણાં ચોરી 2. અંગત ફોટા અને ડેટાની ચોરી 3.બ્લેકમેલિંગ 4. કોન્ટેક્ટ્સને મોર્ફ ફોટા મોકલવાની ધમકી 5. ફોન સંપૂર્ણ હેંગ અથવા બગડી જવો

Anthropicના AI મોડલ “Mythos” અંગે સામે આવેલી માહિતી દર્શાવે છે કે AI માત્ર સાયબર ખામીઓ શોધી શકતું નથી, પરંતુ તેનો કેવી રીતે દુરૂપયોગ કરી શકાય તે માટેના રસ્તા પણ તૈયાર કરી શકે છે – અને તે પણ એવા લોકો માટે જેઓ ટેક્નિકલ નિષ્ણાત નથી.

Mythos I AIની વધતી ચિંતા

સાયબરસિક્યુરિટીની દુનિયામાં ઝડપ સૌથી મહત્વપૂર્ણ ગણાય છે. કોઈપણ સોફ્ટવેરમાં ખામી અથવા વલ્નરેબિલિટી જેટલી ઝડપથી શોધી અને સુધારી શકાય, તેટલો ડેટા વધુ સુરક્ષિત રહે છે. વર્ષો સુધી આ કામ માટે નિષ્ણાતોની મોટી ટીમો અને લાંબા સમયની જરૂર પડતી હતી, પરંતુ હવે આર્ટિફિશિયલ ઇન્ટેલિજન્સ આ પ્રક્રિયાને કલાકોમાં પૂર્ણ કરવાની ક્ષમતા ધરાવે છે. પરંતુ ટેક્નોલોજીની આ જ શક્તિ હવે નવી ચિંતા પણ ઊભી કરી રહી છે. Anthropicના AI મોડલ “Mythos” અંગે સામે આવેલી માહિતી દર્શાવે છે કે AI માત્ર સાયબર ખામીઓ શોધી શકતું નથી, પરંતુ તેનો કેવી રીતે દુરૂપયોગ કરી શકાય તે માટેના રસ્તા પણ તૈયાર કરી શકે છે – અને તે પણ એવા લોકો માટે જેઓ ટેક્નિકલ નિષ્ણાત નથી. ઇન્ટરનેશનલ મોનેટરી ફંડ (IMF)એ ચેતવણી આપી છે કે AI સાયબર સુરક્ષા મજબૂત બનાવવામાં મદદરૂપ બની શકે છે, પરંતુ તે સાયબર હુમલાઓને વધુ ઝડપી, સસ્તા અને સરળ પણ બનાવી શકે છે. ખાસ કરીને બેન્કિંગ, ક્લાઉડ સર્વિસ, પેમેન્ટ નેટવર્ક અને ડિજિટલ ઈન્ફ્રાસ્ટ્રક્ચર પર આધારિત ક્ષેત્રો માટે આ જોખમ વધુ ગંભીર બની શકે છે.Anthropicના “Claude Mythos Preview” મોડલ અંગે કંપનીએ સ્વીકાર્યું કે તે “ઝીરો-ડે” એટલે કે અજાણી અને હજુ સુધી શોધાઈ ન હોય તેવી વલ્નરેબિલિટીઝ શોધી શકે છે. આ AI ઓપન સોર્સ કોડબેઝમાં ખામીઓ શોધવા ઉપરાંત ક્લોઝ્ડ-સોર્સ સોફ્ટવેરમાં રહેલી સુરક્ષા ખામીઓનું વિશ્લેષણ પણ કરી શકે છે.રિપોર્ટ મુજબ Mythos માત્ર ખામી શોધતું નથી, પરંતુ તે ખામીને “એક્સપ્લોઇટ”માં કેવી રીતે ફેરવવી તે અંગેની પ્રક્રિયા પણ સૂચવી શકે છે. Anthropicના એન્જિનિયર્સે દાવો કર્યો કે AIને માત્ર એક રાતમાં સંપૂર્ણ કાર્યરત એક્સપ્લોઇટ તૈયાર કરવા માટે માર્ગદર્શન આપવામાં આવ્યું હતું.

સાયબર સુરક્ષામાં ક્રાંતિ લાવતું AI હવે હેકર્સ માટે પણ બની શકે છે ખતરનાક સાધન

વલ્નરેબિલિટી શોધવાથી લઈને હેકિંગ સુધી : AI હવે સાયબર દુનિયાનો ગેમચેન્જર

AI સામે સાયબર સુરક્ષાની નવી લડાઈ : સરકારો અને નિષ્ણાતોમાં વધતી ચિંતા

સૌથી મોટી ચિંતા એ છે કે Mythos જેવી ક્ષમતાઓ AIને ખાસ હેકિંગ માટે ટ્રેન કર્યા વગર પણ વિકસતી જોવા મળી રહી છે. કંપનીના જણાવ્યા મુજબ આ ક્ષમતાઓ AIની કોડિંગ, રિઝનિંગ અને ઓટોમેશનમાં થયેલા સામાન્ય સુધારાઓના “સાઇડ ઇફેક્ટ” તરીકે ઉભી થઈ છે. નિષ્ણાતો માને છે કે AI આધારિત સાયબર હુમલાઓ ભવિષ્યમાં વધુ સ્કેલેબલ, ઓટોમેટેડ અને સામાન્ય લોકો માટે પણ સુલભ બની શકે છે. એટલે કે હેકિંગ હવે માત્ર નિષ્ણાતોની દુનિયા સુધી મર્યાદિત નહીં રહે.IMFએ વિશ્વભરના સરકારો અને નિયમનકારોને AIને માત્ર ટેક્નિકલ મુદ્દો નહીં પરંતુ “રાષ્ટ્રીય સુરક્ષા” અને “આર્થિક સ્થિરતા” સાથે જોડાયેલા જોખમ તરીકે જોવાની સલાહ આપી છે. ખાસ કરીને નાણાકીય ક્ષેત્ર, ટેલિકોમ, ઊર્જા અને જાહેર સેવાઓ માટે AI આધારિત સાયબર જોખમો વધુ ગંભીર બની શકે છે.ભારતમાં પણ આ મુદ્દે ચિંતા વધી રહી છે. રિપોર્ટ્સ સામે આવ્યા બાદ કે કેટલાક અનધિકૃત યુઝર્સે Mythos સુધી એક્સેસ મેળવી હોઈ શકે છે, કેન્દ્ર સરકારે સાયબર સુરક્ષા અને નાણાકીય ડેટા પર તેના સંભવિત પ્રભાવ અંગે ચર્ચા શરૂ કરી છે. વિશ્લેષકોનું માનવું છે કે વિશ્વ હવે એવા સમય તરફ આગળ વધી રહ્યું છે જ્યાં AI સાયબર સુરક્ષા માટે સૌથી શક્તિશાળી રક્ષણ પણ બની શકે છે અને સૌથી ખતરનાક હુમલાખોર પણ.ટેક્નોલોજી જેટલી વધુ બુદ્ધિશાળી બનશે, તેટલો જ મોટો સવાલ રહેશે – શું માનવ સમાજ તેની ગતિ સાથે સુરક્ષિત રીતે આગળ વધી શકશે?

AI સબ્સ્ક્રિપ્શનનો સવાલ : ખરેખર જરૂર છે કે ફક્ત ડિજિટલ લાલચ?

ChatGPTથી Gemini સુધી–AI ટૂલ્સના પેઈડ પ્લાન્સ લોકોની જરૂરિયાત છે કે ટેક કંપનીઓની નવી કમાણી?

સ્ટ્રીમિંગ પ્લેટફોર્મ્સ બાદ હવે આર્ટિફિશિયલ ઇન્ટેલિજન્સ ક્ષેત્રમાં પણ સબ્સ્ક્રિપ્શન મોડલ ઝડપથી વધતું જઈ રહ્યું છે. OpenAI, Google, Anthropic, Mistral અને xAI જેવી મોટી કંપનીઓ પોતાના AI ટૂલ્સ માટે અલગ અલગ પેઈડ પ્લાન્સ ઓફર કરી રહી છે. શરૂઆતમાં મફતમાં ઉપલબ્ધ રહેલા AI ટૂલ્સ હવે ધીમે ધીમે “પ્રિમિયમ અનુભવ” તરફ ધકેલાઈ રહ્યા છે. આજે ChatGPT Plus, Claude Pro, Gemini Advanced અને અન્ય પ્રીમિયમ AI પ્લાન્સ માટે લોકો દર મહિને 20 ડોલર અથવા વધુ ચૂકવી રહ્યા છે. કેટલીક કંપનીઓ તો 100થી 300 ડોલર સુધીના અદ્યતન પ્લાન્સ પણ ઓફર કરી રહી છે, ખાસ કરીને ડેવલપર્સ અને પ્રોફેશનલ્સ માટે. AI કંપનીઓનું માર્કેટિંગ લગભગ એકસરખું છે – વધુ ઝડપ, વધુ શક્તિશાળી મોડલ, ઓછા પ્રતિબંધો અને અદ્યતન સુવિધાઓ. પરંતુ સવાલ એ છે કે શું સામાન્ય યુઝરને ખરેખર આ બધાની જરૂર છે? ફ્રી વર્ઝન હજુ પણ મોટા ભાગના લોકો માટે પૂરતું સાબિત થઈ રહ્યું છે. Google Geminiનું મફત વર્ઝન Deep Research અને NotebookLM જેવી સુવિધાઓ આપે છે, જ્યારે ChatGPTનું ફ્રી મોડલ GPT-5.3, ઇમેજ જનરેશન અને વેબ સર્ચ જેવી ક્ષમતાઓ સાથે ઉપલબ્ધ છે. Claude અને Mistral પણ મર્યાદિત પરંતુ ઉપયોગી ફ્રી સેવાઓ આપી રહ્યા છે. પ્રાઇવસી અંગે ચિંતિત યુઝર્સ માટે પણ કેટલાક પેઈડ પ્લાન્સ ખાસ આકર્ષક બની રહ્યા છે. ઉદાહરણ તરીકે, Mistral Proમાં “No Telemetry Mode” જેવી સુવિધા છે, જે ડેટા ટ્રેકિંગ અંગે વધુ સુરક્ષા આપવાનો દાવો કરે છે. પરંતુ સામાન્ય યુઝર્સ માટે પરિસ્થિતિ અલગ છે. મોટાભાગના લોકો AIનો ઉપયોગ લેખન, માહિતી શોધ, ઈમેઈલ, સોશિયલ મીડિયા કે સામાન્ય પ્રશ્નોના જવાબ માટે કરે છે – જેમાં ફ્રી વર્ઝન ઘણીવાર પૂરતું સાબિત થાય છે. વિશ્લેષકોનું માનવું છે કે AI કંપનીઓ લોકોમાં “ફ્રી વર્ઝન પૂરતું નથી” એવી માનસિકતા ઊભી કરી રહી છે. મેસેજ લિમિટ, ધીમી સ્પીડ અને મર્યાદિત ઍક્સેસ દ્વારા લોકોને પેઈડ પ્લાન તરફ પ્રોત્સાહિત કરવામાં આવે છે. આમાં એક રસપ્રદ વિરોધાભાસ પણ છે – જેટલી સ્પર્ધા વધે છે, તેટલા ફ્રી AI ટૂલ્સ વધુ સારા બનતા જાય છે. દરેક કંપની વધુ યુઝર્સ ખેંચવા માટે મફત સેવાઓમાં પણ નવી ક્ષમતાઓ ઉમેરતી રહે છે. નિષ્ણાતો સલાહ આપે છે કે જો AI તમારા રોજિંદા વ્યવસાય અથવા પ્રોફેશન માટે જરૂરી ન હોય તો એક સાથે અનેક સબ્સ્ક્રિપ્શન લેવા કરતાં એક યોગ્ય પ્લેટફોર્મ પસંદ કરવું વધુ સમજદારીભર્યું છે. AIનું ભવિષ્ય કદાચ “સબ્સ્ક્રિપ્શન અર્થતંત્ર” તરફ આગળ વધી રહ્યું છે, પરંતુ આજની સ્થિતિમાં સામાન્ય યુઝર માટે ફ્રી AI હજુ પણ ઘણી હદ સુધી પૂરતું અને અસરકારક સાબિત થઈ રહ્યું છે.

કોને ખરેખર ફાયદો? સામાન્ય યુઝર સામે “પાવર યુઝર”ની લડાઈ

ટેક નિષ્ણાતો માને છે કે AIના પેઈડ પ્લાન્સનો સૌથી મોટો ફાયદો ડેવલપર્સ, ડેટા સાયન્ટિસ્ટ્સ અને ટેક્નિકલ પ્રોફેશનલ્સને થાય છે. જે લોકો દરરોજ કોડિંગ, ઓટોમેશન, ડેટા એનાલિસિસ અથવા મોટા પ્રોજેક્ટ્સ પર કામ કરે છે, તેમના માટે AI એજન્ટ્સ મોટી પ્રોડક્ટિવિટી વધારતી ટૂલ બની શકે છે.
Claude Code, ChatGPT Codex અને Google Jules જેવા AI એજન્ટ્સ હવે કોડ લખી શકે છે, બગ ફિક્સ કરી શકે છે, GitHub પર કામ કરી શકે છે અને આખા કોડબેઝનું વિશ્લેષણ કરી શકે છે. કેટલાક AI એજન્ટ્સ તો બેકગ્રાઉન્ડમાં સતત કાર્યરત રહી રાતોરાત ટાસ્ક પૂર્ણ કરવાની ક્ષમતા ધરાવે છે.

Electronic Ink (E Ink) કાગળ જેવી સ્ક્રીનની સ્માર્ટ ટેક્નોલોજી

આજના ડિજિટલ યુગમાં લોકો હવે પુસ્તકો, નોટ્સ અને સમાચાર પણ મોબાઇલ કે ખાસ ડિજિટલ ડિવાઇસમાં વાંચવાનું વધુ પસંદ કરી રહ્યા છે. ખાસ કરીને E-Book Reader તરીકે જાણીતી ડિવાઇસોમાં એક એવી અનોખી ટેક્નોલોજી વપરાય છે જેને E Ink (Electronic Ink) કહેવામાં આવે છે. આ ટેક્નોલોજી સામાન્ય LED અથવા AMOLED સ્ક્રીનથી સંપૂર્ણપણે અલગ છે અને વાંચન માટે ખાસ અનુકૂળ માનવામાં આવે છે.E Ink નો અર્થ Electronic Ink થાય છે. આ એવી ડિસ્પ્લે ટેક્નોલોજી છે જે કાગળ જેવી દેખાય છે. જ્યારે યુઝર E Ink સ્ક્રીન પર વાંચે છે ત્યારે તેને એવું લાગે છે કે જાણે સાચા કાગળ પર લખાણ વાંચી રહ્યા હોય. આ કારણે આંખો પર ઓછો ભાર પડે છે અને લાંબા સમય સુધી વાંચવામાં આરામ મળે છે.E Ink સ્ક્રીનમાં લાખો સૂક્ષ્મ માઇક્રોકેપ્સ્યુલ્સ હોય છે. તેમાં કાળા અને સફેદ રંગના નાનકડા કણો રહેલા હોય છે. જ્યારે વીજ પ્રવાહ આપવામાં આવે છે ત્યારે આ કણો ઉપર કે નીચે ખસે છે અને લખાણ અથવા ચિત્રો બનાવે છે. ખાસ વાત એ છે કે સ્ક્રીન માત્ર પેજ બદલતી વખતે જ વીજળી વાપરે છે. તેથી બેટરીનો વપરાશ ખૂબ ઓછો થાય છે.આ જ કારણ છે કે Amazon Kindle જેવી ડિવાઇસ એક વખત ચાર્જ કર્યા પછી ઘણા દિવસો અથવા ક્યારેક અઠવાડિયા સુધી ચાલે છે. મોબાઇલ અને લેપટોપની સ્ક્રીન સતત લાઇટ છોડે છે, જ્યારે E Ink સ્ક્રીન વધુ કુદરતી અનુભવ આપે છે.

અર્જુન શર્મા
આઈટી એક્સપર્ટ

E Ink શું છે? I E Ink એટલે Electronic Ink ટેક્નોલોજી. આ એવી ખાસ સ્ક્રીન છે જે કાગળ જેવી દેખાય છે અને ખાસ કરીને વાંચન માટે બનાવવામાં આવી છે. સામાન્ય મોબાઇલ સ્ક્રીનની સરખામણીએ તેમાં આંખો પર ઓછો ભાર પડે છે. E Ink સ્ક્રીન લાંબા સમય સુધી વાંચવામાં આરામ આપે છે અને તેમાં બ્લુ લાઇટ પણ ઓછું હોય છે. તેથી વિદ્યાર્થીઓ, પુસ્તકપ્રેમીઓ અને લાંબા સમય સુધી વાંચન કરનાર લોકો માટે આ ટેક્નોલોજી ખૂબ ઉપયોગી માનવામાં આવે છે.

E Ink ની ખાસિયતો I E Ink ટેક્નોલોજીની સૌથી મોટી ખાસિયત તેની લાંબી બેટરી લાઇફ છે. સ્ક્રીન માત્ર પેજ બદલતી વખતે જ વીજળી વાપરે છે, જેના કારણે ડિવાઇસ ઘણા દિવસો સુધી ચાલે છે. ઉપરાંત સૂર્યપ્રકાશમાં પણ સ્ક્રીન સ્પષ્ટ દેખાય છે. તેમાં આંખોને આરામ મળે છે અને સતત વાંચન દરમિયાન થાક ઓછો લાગે છે. આ કારણે Kindle જેવી E-Book Reader ડિવાઇસ વિશ્વભરમાં ખૂબ લોકપ્રિય બની રહી છે.

ક્યાં વપરાય છે? I E Ink ટેક્નોલોજીનો ઉપયોગ હવે ઘણા ક્ષેત્રોમાં થવા લાગ્યો છે. E-Book Reader ઉપરાંત ડિજિટલ નોટબુક, સ્માર્ટ પ્રાઇસ ટેગ અને સ્માર્ટવોચમાં પણ તેનો ઉપયોગ થાય છે. મોટા મોલ અને સ્ટોરમાં ઇલેક્ટ્રોનિક પ્રાઇસ ડિસ્પ્લે માટે E Ink વપરાય છે. શિક્ષણ ક્ષેત્રમાં પણ ડિજિટલ વાંચન અને નોટ્સ માટે આ ટેક્નોલોજી લોકપ્રિય બની રહી છે. ભવિષ્યમાં ઓફિસ અને જાહેર માહિતી ડિસ્પ્લેમાં તેનો ઉપયોગ વધુ વધી શકે છે. E Ink ટેક્નોલોજી વાંચન માટે ઉત્તમ છે, પરંતુ દરેક કામ માટે યોગ્ય નથી.