

૨૧મી સદીમાં સાયબર સુરક્ષાની જરૂરિયાત

આધુનિક યુગને માહિતી અને ટેકનોલોજીનો યુગ કહેવામાં આવે છે. આજે ઇન્ટરનેટ, સ્માર્ટફોન, ક્લાઉડ કમ્પ્યુટિંગ, કૃત્રિમ બુદ્ધિમત્તા (Artificial Intelligence – A.I.), ઓનલાઈન બેંકિંગ અને ડિજિટલ સેવાઓ આપણા જીવનનો અભિન્ન ભાગ બની ગઈ છે. ભારત સહિત સમગ્ર વિશ્વમાં કરોડો લોકો દરરોજ ડિજિટલ માધ્યમોનો ઉપયોગ કરે છે. આવી પરિસ્થિતિમાં વ્યક્તિગત માહિતી, નાણાકીય વ્યવહારો અને સરકારી માહિતીની સુરક્ષા અત્યંત જરૂરી બની છે. આ સુરક્ષાને **સાયબર સુરક્ષા (Cyber Security)** કહેવામાં આવે છે.

સાયબર સુરક્ષાનો અર્થ કમ્પ્યુટર, મોબાઇલ, સર્વર, નેટવર્ક અને ડિજિટલ માહિતીનું હેકિંગ, વાયરસ, માલવેર, રેન્સમવેર, ફિશિંગ અને અન્ય સાયબર હુમલાઓથી રક્ષણ કરવાનો થાય છે. જો યોગ્ય સુરક્ષા ન રાખવામાં આવે તો વ્યક્તિગત માહિતી, બેંક ખાતાની વિગતો, પાસવર્ડ અને મહત્વપૂર્ણ દસ્તાવેજોની ચોરી થઈ શકે છે. તેથી આજના સમયમાં સાયબર સુરક્ષા માત્ર એક ટેકનિકલ જરૂરિયાત નથી, પરંતુ દરેક નાગરિકની જવાબદારી પણ છે.

૨૧મી સદીમાં ડિજિટલ વ્યવહારોમાં નોંધપાત્ર વધારો થયો છે. UPI, નેટ બેંકિંગ, મોબાઇલ વોલેટ અને ઓનલાઈન ખરીદી જેવી સેવાઓએ જીવન સરળ બનાવ્યું છે. પરંતુ તેની સાથે ઓનલાઈન છેતરપિંડીના બનાવોમાં પણ વધારો થયો છે. ઘણી વખત લોકો બોટા ફોન કોલ, નકલી વેબસાઇટ, ફિશિંગ ઈ-મેઇલ અથવા OTP શેર કરવાના કારણે પોતાની મહેનતની કમાણી ગુમાવી બેસે છે. આથી સાયબર સુરક્ષાનું મહત્વ વધુ વધી ગયું છે.

શિક્ષણ ક્ષેત્રમાં પણ સાયબર સુરક્ષા ખૂબ જરૂરી છે. આજે વિદ્યાર્થીઓ ઓનલાઈન અભ્યાસ, પરીક્ષા અને ડિજિટલ લર્નિંગ પ્લેટફોર્મનો ઉપયોગ કરે છે. જો તેમની માહિતી સુરક્ષિત ન રહે તો ડેટા ચોરી, ઓળખની નકલ (Identity Theft) અથવા અન્ય સાયબર ગુનાઓ થઈ શકે છે. તેવી જ રીતે હોસ્પિટલો, બેંકો, ઉદ્યોગો અને સરકારી કચેરીઓમાં લાખો લોકોની માહિતી ડિજિટલ સ્વરૂપમાં સંગ્રહિત હોય છે. આવી માહિતીની સુરક્ષા રાષ્ટ્રીય સુરક્ષા સાથે પણ જોડાયેલી છે.

સાયબર હુમલાઓના ઘણા પ્રકારો છે, જેમ કે હેકિંગ, ફિશિંગ, રેન્સમવેર, માલવેર, સ્પાયવેર અને ડેટા ચોરી. ક્રેટલાક યુનેગારો નકલી વેબસાઇટ અથવા મોબાઇલ એપ બનાવીને લોકોને છેતરે છે. સોશિયલ મીડિયા પર બોટી માહિતી ફેલાવવી, વ્યક્તિગત ફોટા અથવા માહિતીનો દુરુપયોગ કરવો અને ઓનલાઈન બ્લેકમેઇલિંગ જેવી ઘટનાઓ પણ ચિંતાજનક બની રહી છે.

સાયબર સુરક્ષા માટે દરેક વ્યક્તિએ ક્રેટલીક સાવચેતીઓ રાખવી જોઈએ. મજબૂત અને અલગ-અલગ પાસવર્ડનો ઉપયોગ કરવો, સમયાંતરે પાસવર્ડ બદલવો, **Two-Factor Authentication (2FA)** ચાલુ રાખવું, અજાણી લિંક અથવા ઈ-મેઇલ પર ક્લિક ન કરવું, OTP, ATM PIN અથવા બેંકની ગુપ્ત માહિતી કોઈની સાથે શેર ન કરવી તેમજ કમ્પ્યુટર અને મોબાઇલમાં હંમેશા વિશ્વસનીય એન્ટિવાયરસ અને નવીનતમ સોફ્ટવેર અપડેટ રાખવા જોઈએ. સોશિયલ મીડિયા પર પણ વ્યક્તિગત માહિતી મર્યાદિત પ્રમાણમાં જ શેર કરવી જોઈએ.

ભારત સરકાર પણ સાયબર સુરક્ષાને મજબૂત બનાવવા માટે સતત પ્રયાસ કરી રહી છે. **Indian Computer Emergency Response Team (CERT-In)** જેવી સંસ્થા સાયબર હુમલાઓ અંગે ચેતવણી આપે છે અને સાયબર સુરક્ષા માટે માર્ગદર્શન પૂરું પાડે છે. ઉપરાંત, ડિજિટલ ઈન્ડિયા અભિયાન સાથે સુરક્ષિત ડિજિટલ વ્યવહારો અંગે લોકોમાં જાગૃતિ લાવવા માટે વિવિધ કાર્યક્રમો ચલાવવામાં આવે છે.

નિષ્કર્ષ

૨૧મી સદીમાં સાયબર સુરક્ષા માત્ર ટેકનોલોજીનો વિષય નથી, પરંતુ સુરક્ષિત અને જવાબદાર ડિજિટલ જીવન જીવવાનો આધાર છે. જેમ આપણે પોતાના ઘર અને સંપત્તિની સુરક્ષા કરીએ છીએ, તેમ જ પોતાની ડિજિટલ માહિતીનું પણ રક્ષણ કરવું જરૂરી છે. યોગ્ય જાગૃતિ, આધુનિક ટેકનોલોજી અને જવાબદાર વર્તન દ્વારા જ આપણે સાયબર ગુનાઓથી બચી શકીએ. તેથી સાયબર સુરક્ષાને દરેક વ્યક્તિએ પોતાના જીવનનો મહત્વપૂર્ણ ભાગ બનાવવો જોઈએ, કારણ કે **"સુરક્ષિત ડિજિટલ ભારત જ સમૃદ્ધ ભારતનું ભવિષ્ય છે"**